Acerca de esta versión

Novedades

-
-
-
-
-
-
-
-
-
  -
  -
  -
-

-
-
-
-
-

Problemas resueltos en esta versión

Problemas conocidos en esta versión

Problemas resueltos de Citrix Receiver para Windows 4.2

Receiver para Windows 4.2.100

-
-
-
-
  -

-
-
  -
  -
  -
-
-
-
  -
  -
-
-
-

-
-
-
-
-
-
-
-
-
-
-

-
-

Receiver para Windows 4.2

-

-
-
-
-
-
-
-
-

-
-
-
-
-
-
-
-
-
-

-
-
-
-
-
-
-
-
-
-
  -
  -

-
-
-
-
-
-
-
-
-
-
-

-
-
-
-
-
-
-
-
-
-

-
-
-
-
-
-
-
-
-
-
-
-

-
-
  -
  -
  -
  -
-
-
-
-

Problemas conocidos de Citrix Receiver para Windows 4.2

Problemas conocidos

-
-
-
-
-
-
-
-
-

-
-
-
-
-
-
-
-
-

-
-
-

Requisitos del sistema

Dispositivo

Sistema operativo

-
-
-
-
-
-
-
-
-
-

Hardware

-
-
-

Dispositivos de uso táctil

Servidores Citrix

-
  -
  -
  -
  -
  -
  -
-
  -
  -
  -

Browser

Conectividad

-
  -
  -
  -
  -
  -

Acerca de las conexiones seguras y los certificados

Actualizaciones

Otros

-
  -
  -
  -
-
-

-
-

Instalación de Receiver para Windows

-
  -
-
  -
  -
-
  -
-
  -

Actualización manual a Receiver para Windows

-
-
-

-

Consideraciones sobre la actualización

Consideraciones importantes para actualizar desde la versión 3.4 a la versión 4.2.100

Instalación y desinstalación manual de Receiver para Windows

Cómo quitar Receiver para Windows

Configuración e instalación de Receiver para Windows mediante parámetros de línea de comandos

-
-
-
-

-
  -
  -
  -
  -
  -

-
-

-
-
-
-
-
-
-

CitrixReceiver.exe /silent STORE0="AppStore;https://testserver.net/Citrix/MyStore/discovery;on;Almacén de aplicaciones de RRHH"
STORE1="BackUpAppStore;https://testserver.net/Citrix/MyBackupStore/discovery;on;Almacén de respaldo de RRHH"

CitrixReceiver.exe /INCLUDESSON /STORE0="PNAgent;https://testserver.net/Citrix/PNAgent/config.xml;on;My PNAgent Site"

Para iniciar una aplicación o un escritorio virtual desde la línea de comandos

Implementación de Receiver para Windows mediante Active Directory y scripts de inicio de ejemplo

-
-

Para modificar los scripts de ejemplo

-

```
set DesiredVersion= 3.3.0.XXXX
```

-
-
-

Para agregar scripts de inicio de equipo

Para distribuir Receiver por equipos

Para quitar Receiver de equipos particulares

Para configurar scripts de inicio por usuario

-
-

Para distribuir Receiver a usuarios particulares

Para quitar Receiver de usuarios particulares

Implementación de Receiver para Windows desde Receiver para Web

Implementación de Receiver para Windows desde una pantalla de inicio de sesión de la Interfaz Web

Configuración de Receiver para Windows

-
-
-
  -
  -
  -
-
-

Configuración del modo de autoservicio

-
-

Configuración de StoreFront

Configuración de la entrega de aplicaciones

-
-
-

Configuración del modo de autoservicio

-
-

-

Personalización de la ubicación de los accesos directos de las aplicaciones

SelfServiceMode true
SelfServiceMode false

- SelfServiceMode
false
-
-
-
- UseCategoryAsStartMenuPath
- [/DESKTOPDIR="nombre de directorio"]
CategoryPath
-
AutoReInstallModifiedApps

Uso de la plantilla de objetos de directiva de grupo para personalizar las ubicaciones de los accesos directos de aplicaciones

-
-
-
-
-
-
-

Uso de las claves del Registro para personalizar las ubicaciones de los accesos directos de las aplicaciones

Uso de los parámetros de cuenta de StoreFront para personalizar las ubicaciones de los accesos directos de aplicaciones

-
-
-

-
-
-
-
-

Uso de los parámetros de aplicación en XenApp y XenDesktop 7.x para personalizar las ubicaciones de los accesos directos de las aplicaciones

Uso de los parámetros de aplicación en XenApp 7.6 para personalizar las ubicaciones de los accesos directos de las aplicaciones

Disminuir las demoras de enumeración o firma digital de código auxiliar de aplicaciones

Ejemplo de casos de uso

Configuración de aplicaciones para el acceso a aplicaciones locales

-

- -

-

-

-

Configuración del entorno de XenDesktop

Configuración del respaldo para USB en conexiones de XenDesktop y XenApp

•

Funcionamiento del respaldo USB

Dispositivos de almacenamiento masivo

Clases de dispositivos USB que se admiten de manera predeterminada

-
-
-
-
-
    -
    -
    -
    -
    -
    -
-

-
-
-

Clases de dispositivos USB que se rechazan de manera predeterminada

-
-
-
-
-
-
-

Actualización de la lista de dispositivos USB que se encuentran disponibles para la comunicación remota

Configuración de teclados Bloomberg

-
-

Impedir que la ventana de Desktop Viewer se atenúe

-
-

-
-

Para configurar parámetros para varios usuarios y dispositivos

-

-
-

Configuración de StoreFront

Para configurar StoreFront

Configuración de Receiver con la plantilla de objeto de directiva de grupo

-
-
-
-

AlmacenVentas;https://ventas.ejemplo.com/Citrix/Store/discovery;On;Almacén para el personal de Ventas

Cómo proporcionar información de cuentas a los usuarios

-
-
-

Configuración de la detección de cuentas basada en direcciones de correo electrónico

Entrega de un archivo de aprovisionamiento a los usuarios

-

Entrega de la información de cuenta para introducirla manualmente

-

-
  -
  -

    NetScalerGatewayFQDN?MyStoreName

Optimización del entorno de Receiver

Reducción del tiempo de inicio de las aplicaciones

-
-

-
-

Valores de Registro HKLM

Valores de Registro HKCU

Asignación de dispositivos del cliente

-
-
-

Desactivar la asignación de dispositivos de usuario

Redirección de carpetas del cliente

Asignación de unidades del cliente a letras de unidad del host

Redirección de dispositivos USB de HDX Plug and Play

Para asignar un puerto COM del cliente a un puerto COM del servidor

Respaldo para resolución de nombres DNS

Para inhabilitar la resolución de nombres DNS para dispositivos cliente específicos

Utilización de servidores proxy con conexiones de XenDesktop

Dec 03, 2015

Si no utiliza servidores proxy en su entorno, corrija los parámetros de proxy de Internet Explorer en los dispositivos de usuario que ejecutan Internet Explorer 7.0 con Windows XP. De manera predeterminada, esta configuración detecta automáticamente los parámetros de proxy. Si no se utilizan servidores proxy, los usuarios experimentarán demoras innecesarias durante el proceso de detección. Para obtener instrucciones para modificar los parámetros de proxy, consulte la documentación de Internet Explorer. O bien, puede modificar los parámetros de proxy mediante la Interfaz Web. Para más información, consulte la documentación de la Interfaz Web.

Mejora de la experiencia del usuario

Nov 19, 2015

Es posible mejorar la experiencia de uso mediante las siguientes funciones:

Receiver admite varias entradas de micrófono en el cliente. Los micrófonos instalados localmente se pueden usar para:

- Actividades en tiempo real, como llamadas desde sistemas de telefonía integrada en el equipo y conferencias Web.
- Aplicaciones de grabación en el servidor, como programas de dictado.
- Grabaciones de vídeo y sonido.

Los usuarios de Receiver pueden seleccionar si quieren usar los micrófonos conectados a sus dispositivos, cambiando un parámetro en la Central de conexiones. Los usuarios de XenDesktop también pueden usar las Preferencias de XenDesktop Viewer para inhabilitar sus micrófonos y cámaras Web.

Se pueden usar hasta ocho monitores con Receiver.

Las sesiones pueden distribuirse entre varios monitores de dos formas:

- En modo de pantalla completa, con varios monitores en la sesión; las aplicaciones se presentan en los monitores como lo harían localmente.
  XenDesktop: Puede mostrar la ventana de Desktop Viewer en cualquier subconjunto rectangular de monitores; para ello, cambie el tamaño de la ventana en cualquier parte de los monitores y presione el botón Maximizar.
- En modo de ventanas, con un única imagen de monitor para la sesión; las aplicaciones no se muestran en monitores individuales.

XenDesktop: cuando posteriormente se inicia cualquier escritorio en la misma asignación (anteriormente "grupo de escritorios"), se mantiene el parámetro de ventana y se muestra el escritorio en los mismos monitores. En la medida en que la distribución de monitores sea rectangular, se pueden mostrar varios escritorios virtuales en un dispositivo. Si la sesión de XenDesktop usa el monitor principal en el dispositivo, éste será el monitor principal de la sesión. De lo contrario, el monitor con el número más bajo en la sesión se convierte en el monitor principal.

Para habilitar el respaldo de varios monitores, asegúrese de lo siguiente:

- El dispositivo de usuario está configurado para respaldar el uso de varios monitores.
- El sistema operativo del dispositivo de usuario debe ser capaz de detectar cada monitor. Para verificar que esta detección ocurre en el dispositivo de usuario en las plataformas Windows, confirme que cada monitor aparece por separado en la ficha Configuración del cuadro de diálogo Configuración de pantalla.
- Después de detectar los monitores:
  - **XenDesktop:** Configure el límite de memoria gráfica con el parámetro Límite de memoria de presentación de Directivas de equipo Citrix.
  - **XenApp:** Según la versión del servidor XenApp que tenga instalada:
    - Configure el límite de memoria gráfica con el parámetro Límite de memoria de presentación de Directivas de equipo Citrix.
    - En la consola de administración Citrix del servidor XenApp, seleccione la comunidad y, en el panel de tareas, seleccione Modificar las propiedades del servidor > Modificar todas las propiedades > Predeterminadas del servidor

> HDX Broadcast > Presentación (o Modificar las propiedades del servidor > Modificar todas las propiedades > Predeterminadas del servidor > ICA > Presentación) y configure el parámetro Memoria máxima a utilizar para los gráficos de cada sesión (KB).

Asegúrese de que el parámetro es lo suficientemente amplio (en kilobytes) para ofrecer suficiente memoria gráfica. Si este parámetro no es lo suficientemente grande, el recurso publicado se restringirá al subconjunto de monitores que cubra el tamaño especificado.

Para obtener información sobre el cálculo de los requisitos de memoria gráfica de XenApp y XenDesktop, consulte ctx115637.

Si en la configuración de directiva Valores predeterminados de optimización de impresión universal está habilitada la opción Permitir a los no administradores modificar estos parámetros, los usuarios pueden anular las opciones Compresión de imágenes y Almacenamiento en caché de imágenes y fuentes especificadas en esa configuración de directiva.

Para sobrescribir los parámetros de la impresora en el dispositivo de usuario

1. En el menú Imprimir de la aplicación del dispositivo de usuario, elija Propiedades.
2. En la ficha Parámetros del cliente, haga clic en Optimizaciones avanzadas y realice cambios a las opciones Compresión de imagen y Almacenamiento en caché de imágenes y fuentes.

Para habilitar el acceso táctil a las aplicaciones y escritorios virtuales desde tabletas Windows, Receiver muestra automáticamente el teclado en pantalla al activar un campo de entrada de texto, y cuando el dispositivo está en modo tienda o tableta.

En algunos dispositivos y en algunas circunstancias, Receiver no puede detectar el modo en que se encuentra un dispositivo, y es posible que el teclado en pantalla aparezca cuando no sea necesario.

Para impedir que aparezca el teclado en pantalla al usar un dispositivo convertible (tableta con teclado extraíble), cree un valor de REG_DWORD con DisableKeyboardPopup en HKLM\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\MobileReceiver y establezca el valor en 1.
Nota: En una máquina x64, cree el valor en HKLM\SOFTWARE\Wow6432Node\ Citrix\ICA Client\Engine\Configuration\Advanced\Modules\MobileReceiver

Se pueden configurar combinaciones de teclas para que Receiver las interprete como una funcionalidad especial. Cuando se habilita la directiva de teclas de acceso directo, se pueden especificar las teclas de acceso directo de Citrix, el comportamiento de las teclas de acceso directo de Windows y la disposición del teclado para las sesiones.

1. Como administrador, abra el Editor de directivas de grupo mediante la ejecución de gpedit.msc localmente desde el menú Inicio si va a aplicar directivas para un solo equipo, o bien, mediante la Consola de administración de directivas de grupo si va a aplicar directivas de dominio.

   Nota: Si ya importó la plantilla icaclient al Editor de directivas de grupo, puede omitir los pasos 2 a 5.
2. En el panel izquierdo del Editor de directivas de grupo, seleccione la carpeta Plantillas administrativas.
3. En el menú Acción, seleccione Agregar o quitar plantillas.
4. Seleccione Agregar y vaya a la carpeta Configuration de Receiver (normalmente C:\Archivos de programa\Citrix\ICA

Client\Configuration) y seleccione icaclient.adm.
5. Seleccione Abrir para agregar la plantilla y luego, haga clic en Cerrar para regresar al Editor de directivas de grupo.
6. En el Editor de directivas de grupo, vaya a Plantillas administrativas > Plantillas administrativas clásicas (ADM) > Citrix Components > Citrix Receiver > User Experience > Keyboard shortcuts.
7. En el menú Acción, elija Propiedades, seleccione Habilitada y luego elija las opciones deseadas.

Receiver respalda los iconos de color de alta densidad (de 32 bits) y selecciona automáticamente la profundidad de color de las aplicaciones que se muestran en el cuadro de diálogo Central de conexiones de Citrix, en el menú Inicio y en la barra de tareas para proporcionar una integración total.

Precaución: Si edita el Registro de forma incorrecta podrían generarse problemas graves que pueden hacer que sea necesario instalar nuevamente el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Asegúrese de hacer una copia de seguridad del registro antes de modificarlo.
Para establecer una profundidad preferida, se puede agregar la clave de Registro TWIDesiredIconColor a HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Preferences y establecerla en el valor deseado. Las profundidades de color posibles son 4, 8, 16, 24 y 32 bits por píxel. Si la conexión de la red es lenta, los usuarios pueden seleccionar valores de profundidad de color menores para los iconos.

Cada empresa tiene sus propias necesidades de negocio. Los requisitos para el acceso por parte de los usuarios a los escritorios virtuales pueden variar de usuario a usuario y a medida que evolucionan las necesidades de la empresa. La experiencia del usuario a la hora de conectarse con los escritorios virtuales, así como su interacción en la configuración de las conexiones depende de cómo se configure Receiver para Windows.

Use **Desktop Viewer** cuando los usuarios necesiten interactuar con el escritorio virtual. El escritorio virtual del usuario pueden ser un escritorio virtual publicado, o un escritorio compartido o escritorio dedicado. En este modo de acceso, las funciones de la barra de herramientas de Desktop Viewer permiten al usuario abrir un escritorio virtual en una ventana y, desplazar y cambiar el tamaño de ese escritorio dentro del escritorio local. Los usuarios pueden definir preferencias y conectarse con más de un escritorio utilizando varias conexiones XenDesktop en el mismo dispositivo de usuario.

Nota: Los usuarios deben usar Citrix Receiver para cambiar la resolución de pantalla en sus escritorios virtuales. No pueden cambiar la resolución de pantalla usando el Panel de control de Windows.

En las sesiones de Desktop Viewer, la combinación de la tecla con el logotipo de Windows+L se transfiere al equipo local.

Ctrl+Alt+Supr se transfiere al equipo local.

Las pulsaciones de teclas que activan StickyKeys, FilterKeys y ToggleKeys (características de accesibilidad de Microsoft) siempre se transfieren al equipo local.

Como una funcionalidad de accesibilidad de Desktop Viewer, al presionar Ctrl+Alt+Interrumpir se muestran los botones de la barra de herramientas de Desktop Viewer en una ventana emergente.

Ctrl+Esc se envía al escritorio virtual remoto.

Nota: De forma predeterminada, Alt+Tab transfiere el foco entre las ventanas de la sesión si Desktop Viewer está maximizado. Si Desktop Viewer se muestra en una ventana, Alt+Tab transfiere el foco entre las ventanas fuera de la sesión.

Las secuencias de teclas de acceso rápido son combinaciones de teclas diseñadas por Citrix. Por ejemplo, la secuencia Ctrl+F1 reproduce las teclas Ctrl+Alt+Supr, y Mayús+F2 cambia entre el modo de pantalla completa y de ventanas en las aplicaciones. No puede usar las secuencias de teclas de acceso rápido con escritorios virtuales que se muestran en Desktop Viewer (en sesiones de XenDesktop), pero puede usarlas con aplicaciones publicadas (en sesiones de XenApp).

Los usuarios no pueden conectarse con el mismo escritorio virtual desde una sesión de escritorio. Si se intenta, se desconectará la sesión de escritorio existente. Por lo tanto, Citrix recomienda lo siguiente:

- Los administradores no deben configurar a los clientes de un escritorio para que se conecten con un sitio que publica el mismo escritorio.
- Los usuarios no deben buscar un sitio que aloje el mismo escritorio si el sitio se configura para reconectar a los usuarios automáticamente con las sesiones existentes.
- Los usuarios no deben buscar un sitio que aloje el mismo escritorio e intentar ejecutarlo.

Tenga en cuenta que un usuario que inicia una sesión localmente en un equipo que actúa como escritorio virtual bloquea las conexiones con ese escritorio.

Si los usuarios se conectan con aplicaciones virtuales (publicadas con XenApp) desde un escritorio virtual y la organización dispone de un administrador de XenApp independiente, Citrix sugiere aunar esfuerzos para definir la asignación de dispositivos para que los dispositivos de escritorio se asignen siempre dentro de las sesiones de aplicación y escritorio. Debido a que las unidades locales se muestran como unidades de red en las sesiones de escritorio, el administrador de XenApp necesita modificar la directiva de asignación de unidades para que incluya las unidades de red.

Protección de las conexiones

Nov 19, 2015

Para maximizar la seguridad del entorno, las conexiones entre Receiver y los recursos que se publiquen deben ser seguras. Puede configurar diversos tipos de autenticación para el software de Receiver, incluidos: autenticación con tarjeta inteligente, comprobación de lista de revocación de certificados y autenticación PassThrough con Kerberos.

La autenticación mediante Desafío/Respuesta de Windows NT (NTLM) recibe respaldo de manera predeterminada en los equipos Windows.

Configuración de autenticación PassThrough de dominio

Dec 03, 2015

Este tema explica cómo habilitar la autenticación PassThrough de dominio para Citrix Receiver con XenDesktop o XenApp.

Nota: En este ejemplo, la instalación de Receiver, la aplicación de directivas de equipo y la configuración de un sitio de confianza en el sistema operativo del cliente se llevan a cabo manualmente. Una vez creada una plantilla de objeto de directiva de grupo (GPO), se la puede aplicar a cualquier máquina cliente del dominio que tenga instalado Receiver.

1. Instale Citrix Receiver 4.2 con la opción /includeSSON.
    1. Instale uno o varios almacenes de StoreFront. Puede completar este paso más adelante. La instalación de almacenes de StoreFront no es un requisito previo para configurar la autenticación PassThrough de dominio. Para obtener información acerca de la sintaxis para agregar uno o varios almacenes de StoreFront, consulte Configuración e instalación de Receiver para Windows mediante parámetros de línea de comandos.
    2. Compruebe si la autenticación PassThrough está habilitada iniciando Citrix Receiver y viendo si el proceso **ssonsvr.exe** se está ejecutando.
2. Agregue la plantilla administrativa de GPO del Cliente ICA a la directiva de equipo local en la máquina local del usuario y/o en la imagen maestra del escritorio VDA:
    1. Abra **gpedit.msc**.
       Nota: El complemento del Editor de directivas de grupo, gpedit.msc, está disponible en las ediciones Professional, Enterprise y Ultimate de Windows 7 y Windows 8.
    2. Haga clic con el botón secundario en Configuración del equipo > Plantillas administrativas y seleccione Agregar o quitar plantillas.
    3. Agregue la plantilla **C:\Archivos de programa\Citrix\ICA Client\Configuration\icaclient.adm**.
3. Habilite el siguiente GPO de equipo local en la máquina local del usuario y/o en la imagen maestra del escritorio VDA:
    1. Seleccione Local user name and password.
    2. Seleccione Habilitada.
    3. Seleccione Enable pass-through authentication.
    4. Seleccione Allow pass-through authentication for all ICA connections.
    5. Haga clic en Aceptar.
    6. Reinicie la imagen maestra del escritorio VDA.
4. Inicie una sesión en los Delivery Controllers, abra Windows PowerShell y ejecute los siguientes comandos para permitir que el Delivery Controller confíe en las solicitudes XML enviadas desde StoreFront.
    1. Si aún no los ha cargado, cargue los cmdlets de Citrix; para ello, escriba asnp Citrix*. (asegúrese de incluir el punto final después de Citrix*).
    2. Presione Entrar.
    3. A continuación, escribaAdd-PSSnapin citrix.broker.admin.v2 y presione INTRO.
    4. A continuación, escribaSet-BrokerSite -TrustRequestsSentToTheXmlServicePort $True y presione INTRO.
    5. Cierre PowerShell.
5. Abra Internet Explorer en la máquina local y/o la imagen maestra del escritorio VDA.
6. En Opciones de Internet > Seguridad > Sitios de confianza, agregue a la lista el nombre FQDN de los servidores StoreFront, sin la ruta del almacén. Por ejemplo: https://storefront.example.com
   Nota: También puede agregar el servidor StoreFront a los Sitios de confianza usando un GPO de Microsoft. El GPO se llama Lista de asignación de sitio a zona y la encontrará en Configuración del equipo > Plantillas administrativas > Componentes de Windows > Internet Explorer > Panel de control de Internet > Página Seguridad.

7. Cierre la sesión y vuelva a iniciarla en Receiver.

Cuando se abre Citrix Receiver, si el usuario actual tiene una sesión iniciada en el dominio, sus credenciales de usuario se transferirán a StoreFront y se enumerarán las aplicaciones y escritorios dentro de Citrix Receiver, además del menú Inicio del usuario. Cuando el usuario hace clic en un icono, Receiver transfiere las credenciales de dominio del usuario al Delivery Controller y la aplicación o el escritorio seleccionados se abren.

Habilitación de la autenticación PassThrough cuando los sitios no se encuentran en sitios de confianza o zonas Intranet

Dec 03, 2015

Es posible que los usuarios requieran autenticación PassThrough (de paso de credenciales) al servidor con sus credenciales de inicio de sesión de usuario, pero no podrán agregar sitios a las zonas Sitios de confianza o Intranet. Habilite este parámetro para permitir la autenticación PassThrough en todos los sitios excepto los restringidos.

1. Como administrador, abra el Editor de directivas de grupo mediante la ejecución de gpedit.msc localmente desde el menú Inicio si va a aplicar directivas para un solo equipo, o bien, mediante la Consola de administración de directivas de grupo si va a aplicar directivas de dominio.
   Nota: Si ya importó la plantilla icaclient al Editor de directivas de grupo, puede omitir los pasos 2 a 5.
2. En el panel izquierdo del Editor de directivas de grupo, seleccione la carpeta Plantillas administrativas.
3. En el menú Acción, seleccione Agregar o quitar plantillas.
4. Seleccione Agregar y vaya a la carpeta Configuration de Receiver (normalmente C:\Archivos de programa\Citrix\ICA Client\Configuration) y seleccione icaclient.adm.
5. Seleccione Abrir para agregar la plantilla y luego, haga clic en Cerrar para regresar al Editor de directivas de grupo.
6. En el Editor de directivas de grupo, vaya a Plantillas administrativas > Plantillas administrativas clásicas (ADM) > Citrix Components > Citrix Receiver > User authentication > Local user name and password.
7. En el menú de Propiedades de Local user name and password, seleccione Habilitada y después seleccione las casillas Enable pass-through authentication y Allow pass-through authentication for all ICA connections.

Configuración de autenticación PassThrough de dominio con Kerberos

Dec 03, 2015

Este tema se aplica solo a conexiones entre Receiver y StoreFront, XenDesktop o XenApp.

Receiver para Windows respalda Kerberos para la autenticación PassThrough de dominio en implementaciones que usan tarjetas inteligentes. Kerberos es uno de los métodos de autenticación incluidos en la autenticación de Windows integrada (IWA).

Cuando la autenticación Kerberos está habilitada, Kerberos autentica sin contraseña para Receiver, y así impide ataques de tipo troyano que intentan tener acceso a las contraseñas del dispositivo de usuario. Los usuarios pueden iniciar una sesión en el dispositivo de usuario con cualquier método de autenticación; por ejemplo, un autenticador biométrico, tal como un lector de huellas digitales, y aún acceder a los recursos publicados sin necesidad de otra autenticación.

Receiver gestiona la autenticación PassThrough con Kerberos del siguiente modo, cuando Receiver, StoreFront, XenDesktop y XenApp están configurados para usar autenticación con tarjeta inteligente y el usuario inicia una sesión con una de ellas:

1. El servicio Single Sign-On de Receiver captura el PIN de la tarjeta inteligente.
2. Receiver usa IWA (Kerberos) para autenticar al usuario en StoreFront. A continuación, StoreFront entrega a Receiver la información referente a las aplicaciones y escritorios virtuales disponibles.
   Nota: No tiene que usar autenticación Kerberos para este paso. Solo se necesita habilitar Kerberos en Receiver para evitar que se vuelva a pedir el PIN. Si no usa la autenticación Kerberos authentication, Receiver autentica en StoreFront usando las credenciales de la tarjeta inteligente.
3. El motor de HDX (antes conocido como cliente ICA) pasa el PIN de la tarjeta inteligente a XenDesktop o XenApp para iniciar la sesión Windows del usuario. A continuación, XenDesktop o XenApp entregan los recursos solicitados.

Para usar autenticación Kerberos con Receiver, asegúrese de que la configuración de Kerberos cumple lo siguiente.

- Kerberos solo funciona entre Receiver y servidores que pertenecen a los mismos dominios de Windows o a dominios que son de confianza. Los servidores también deben ser fiables para la delegación, una opción que se configura mediante la herramienta de administración de usuarios y equipos de Active Directory.
- Kerberos debe estar habilitado en el dominio y en XenDesktop y XenApp. Para mayor seguridad y para asegurarse de que se utiliza Kerberos, inhabilite las demás opciones que no sean Kerberos IWA en el dominio.
- El inicio de sesión con Kerberos no está disponible para conexiones de Servicios de escritorio remoto configuradas para usar autenticación Básica, para usar siempre la información de inicio de sesión especificada o para pedir siempre una contraseña.

El resto de este tema describe cómo configurar la autenticación PassThrough de dominio para los escenarios de uso más frecuentes. Si migra a StoreFront desde la Interfaz Web y previamente utilizó una solución de autenticación personalizada, póngase en contacto con un representante del servicio de asistencia de Citrix Support para obtener más información.

Precaución: Parte de la configuración descrita en este tema incluye modificaciones del Registro. El uso incorrecto del Editor del Registro del sistema puede causar problemas graves que pueden requerir la reinstalación del sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Asegúrese de hacer una copia de seguridad del Registro antes de

editarlo.

Si no está familiarizado con implementaciones de tarjeta inteligente en un entorno XenDesktop, le recomendamos que consulte la información sobre tarjetas inteligentes que figura en la sección Protección de la seguridad del entorno de la documentación de XenDesktop antes de continuar.

Cuando instale Receiver, incluya la opción siguiente en la línea de comandos:

- /includeSSON
  Esta opción instala el componente Single Sign-on en el equipo unido a un dominio, lo que habilita a Receiver para autenticarse en StoreFront usando IWA (Kerberos). El componente Single Sign-on guarda el PIN de la tarjeta inteligente, que luego es utilizado por el motor HDX cuando comunica de forma remota el hardware de tarjeta inteligente y las credenciales a XenDesktop. XenDesktop selecciona automáticamente un certificado desde la tarjeta inteligente y obtiene el PIN desde el motor de HDX.

  Hay una opción relacionada, ENABLE_SSON, que está habilitada de manera predeterminada y debe dejarse así.

  Si hay una directiva de seguridad que impide la habilitación del Single Sign-on en un dispositivo, configure Receiver con la directiva siguiente:

  Plantillas administrativas > Plantillas administrativas clásicas (ADM) > Citrix Components > Citrix Receiver > User authentication > Local user name and password

  Nota: En este caso, usted quiere permitir que el motor de HDX use la autenticación de tarjeta inteligente y no Kerberos, de modo que no use la opción ENABLE_KERBEROS=Yes, ya que forzaría al motor de HDX a usar Kerberos.

Para aplicar la configuración, reinicie Receiver en el dispositivo del usuario.

Para configurar StoreFront:

- En el archivo default.ica ubicado en el servidor StoreFront, defina DisableCtrlAltDel con el valor false.
  Nota: Este paso no es necesario si todas las máquinas cliente ejecutan Receiver para Windows versión 4.2 o posterior.
- Cuando configure el servicio de autenticación en el servidor StoreFront, marque la casilla PassThrough de dominio. Este parámetro habilita la autenticación de Windows integrada (IWA). No es necesario marcar la casilla Tarjeta inteligente a menos que también tenga clientes que no estén unidos a un dominio conectándose a StoreFront con tarjeta inteligente.

Para obtener más información sobre el uso de tarjetas inteligentes con StoreFront, consulte Configuración del servicio de autenticación en la documentación de StoreFront.

Configuración de la autenticación con tarjeta inteligente

Dec 03, 2015

Receiver para Windows respalda las siguientes funciones de autenticación con tarjeta inteligente. Para obtener información sobre la configuración de XenDesktop y StoreFront, consulte la documentación de esos componentes. Este tema describe la configuración de Receiver para Windows para usar tarjetas inteligentes.

- **Autenticación PassThrough (Single Sign-on)**: La autenticación PassThrough captura las credenciales de la tarjeta inteligente cuando los usuarios inician una sesión en Receiver. Receiver usa de este modo las credenciales capturadas:
  - Los usuarios de dispositivos que pertenecen a un dominio que inician una sesión en Receiver usando una tarjeta inteligente pueden iniciar aplicaciones y escritorios virtuales sin necesidad de volver a autenticarse.
  - Los usuarios de dispositivos que no pertenecen a un dominio que inician una sesión en Receiver usando una tarjeta inteligente deben introducir de nuevo sus credenciales para poder iniciar aplicaciones y escritorios virtuales.

  La autenticación PassThrough requiere una configuración de StoreFront y Receiver.

- **Autenticación bimodal**: La autenticación bimodal ofrece a los usuarios la opción de usar una tarjeta inteligente o introducir su nombre de usuario y contraseña. Esta función resulta útil cuando no se puede usar la tarjeta inteligente por alguna razón (por ejemplo, si el usuario la olvidó en casa o el certificado de inicio de sesión caducó). Para permitir esto, deben configurarse almacenes dedicados para cada sitio, usando el método DisableCtrlAltDel con el valor False para permitir tarjetas inteligentes. La autenticación bimodal requiere una configuración de StoreFront. Si hay un dispositivo NetScaler Gateway en la implementación, también será necesario configurarlo.
  Con la autenticación bimodal, administrador de StoreFront tiene ahora la oportunidad de ofrecer al usuario la posibilidad de autenticarse con nombre y contraseña o con tarjeta inteligente en un mismo almacén, seleccionando estas opciones en la consola de StoreFront. Consulte la documentación de StoreFront.

- **Varios certificados:** Puede haber varios certificados disponibles para una única tarjeta inteligente y si se utilizan varias tarjetas inteligentes. Cuando un usuario introduce una tarjeta inteligente en el lector de tarjetas, los certificados están disponibles para todas las aplicaciones ejecutadas en el dispositivo del usuario, incluido Receiver. Para cambiar cómo se seleccionan los certificados, configure Receiver.
- **Autenticación por certificado del cliente**: La autenticación por certificado del cliente requiere la configuración de NetScaler Gateway/Access Gateway y StoreFront.
  - Para acceder a los recursos de StoreFront a través de NetScaler Gateway/Access Gateway, es posible que los usuarios tengan que volver a autenticarse después de extraer una tarjeta inteligente.
  - Cuando la configuración SSL de NetScaler Gateway/Access Gateway está definida como autenticación por certificado de cliente obligatoria, la operación es más segura. No obstante, la autenticación por certificado de cliente obligatoria no es compatible con la autenticación bimodal.
- **Sesiones de doble salto**: Si es necesario el doble salto, se establece una conexión adicional entre Receiver y el escritorio virtual del usuario. Las implementaciones que respaldan el doble salto se describen en la documentación de XenDesktop.
- **Aplicaciones habilitadas para el uso de tarjeta inteligente**: Las aplicaciones habilitadas para tarjeta inteligente, como Microsoft Outlook y Microsoft Office, permiten a los usuarios firmar digitalmente o cifrar documentos disponibles en las sesiones de aplicación o escritorio virtual.

Requisitos previos

Este tema presupone que el lector conoce los temas sobre tarjetas inteligentes en la documentación de XenDesktop y StoreFront.

Limitaciones

- Los certificados deben guardarse en una tarjeta inteligente, no en el dispositivo del usuario.
- Receiver para Windows no guarda la elección de certificado del usuario, pero puede guardar el PIN si se configura así. El PIN solo se almacena en caché en la memoria no paginada durante la sesión del usuario. No se guarda en disco en ningún momento.
- Receiver para Windows no reconecta sesiones cuando se introduce una tarjeta inteligente.
- Cuando está configurado para la autenticación con tarjeta inteligente, Receiver para Windows no respalda Single Sign-on en redes privadas virtuales (VPN) ni el preinicio de sesiones. Para usar túneles VPN con autenticación con tarjeta inteligente, los usuarios deben instalar el NetScaler Gateway Plug-in e iniciar una sesión a través de una página Web, usando sus tarjetas inteligentes y números PIN para autenticarse en cada paso. La autenticación PassThrough en StoreFront con NetScaler Gateway Plug-in no está disponible para los usuarios de tarjeta inteligente.
- Las comunicaciones de Receiver para Windows Updater con citrix.com y Merchandising Server no son compatibles con la autenticación con tarjeta inteligente en NetScaler Gateway.

Precaución: Parte de la configuración descrita en este tema incluye modificaciones del Registro. El uso incorrecto del Editor del Registro del sistema puede causar problemas graves que pueden requerir la reinstalación del sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Asegúrese de hacer una copia de seguridad del Registro antes de editarlo.

Para configurar Receiver, incluya la siguiente opción de línea de comandos cuando lo instale:

- ENABLE_SSON=Yes
  Single sign-on es otro término para autenticación PassThrough. Cuando se habilita este parámetro Receiver no muestra una segunda petición de PIN al usuario.

O, puede realizar la configuración a través de esta directiva y unos cambios en el Registro:

- Plantillas administrativas > Plantillas administrativas clásicas (ADM) > Citrix Components > Citrix Receiver > User authentication > Local user name and password
- Configure SSONCheckEnabled con el valor false en cualquiera de estas claves de Registro si el componente Single Sign-on no está instalado. La clave impide que el Authentication Manager en Receiver compruebe el componente Single Sign-on, lo que permite a Receiver autenticarse con StoreFront.
  HKEY_CURRENT_USER\Software\Citrix\AuthManager\protocols\integratedwindows\

  HKEY_LOCAL_MACHINE\Software\Citrix\AuthManager\protocols\integratedwindows\

De forma alternativa, es posible habilitar la autenticación con tarjeta inteligente en StoreFront en lugar de Kerberos. Para habilitar la autenticación con tarjeta inteligente en StoreFront en lugar de Kerberos, instale Receiver con las opciones de la línea de comandos que se muestran más abajo. Esto requiere privilegios de administrador. La máquina no necesita estar unida a un dominio.

- /includeSSON instala Single Sign-on (autenticación PassThrough). Habilita el almacenamiento en caché de credenciales y el uso de la autenticación PassThrough de dominio.
- Si el usuario está iniciando una sesión en el punto final con otro método distinto de la tarjeta inteligente para la

autenticación en Receiver (por ejemplo, con nombre de usuario y contraseña), la línea de comandos es:
/includeSSON LOGON_CREDENTIAL_CAPTURE_ENABLE=No
Esto evita que se capturen las credenciales al iniciar la sesión y permite a Receiver guardar el PIN al iniciar una sesión en Receiver.

- Vaya a Directiva > Plantillas administrativas > Plantillas administrativas clásicas (ADM) > Citrix Components > Citrix Receiver > User authentication > Local user name and password
  Enable pass-through authentication. Dependiendo de la configuración y los parámetros de seguridad, puede que tenga que seleccionar la opción Allow pass-through authentication for all ICA para que la autenticación PassThrough funcione.

Para configurar StoreFront:

- Al configurar el servicio de autenticación, marque la casilla Tarjeta inteligente.

Para obtener más información sobre el uso de tarjetas inteligentes con StoreFront, consulte Configuración del servicio de autenticación en la documentación de StoreFront.

1. Importe el certificado raíz de la entidad de certificación en el almacén de claves del dispositivo.
2. Instale el middleware de su proveedor de servicios criptográficos.
3. Instale y configure Receiver para Windows.

De manera predeterminada, si hay varios certificados que son válidos, Receiver pide al usuario que elija uno de la lista. De manera alternativa, puede configurar Receiver para usar el certificado predeterminado (según lo indique el proveedor de la tarjeta inteligente) o el certificado con la fecha de caducidad más lejana. Si no hay certificados de inicio de sesión válidos, se notifica esto al usuario y se le da la opción de usar un método de inicio de sesión alternativo, si hay alguno disponible.

Un certificado válido debe reunir estas características:

- La fecha y hora actuales según el reloj del equipo local está dentro del periodo de validez del certificado.
- La clave pública Sujeto debe usar el algoritmo de RSA y tener una longitud de 1024, 2048 ó 4096 bits.
- El campo Uso de la clave debe contener Firma digital.
- El Nombre alternativo del sujeto debe contener el nombre principal del usuario (UPN).
- El campo Uso mejorado de claves debe contener Inicio de sesión de tarjeta inteligente y Autenticación del cliente o Todos los usos de la clave.
- Una de las entidades de certificación en la cadena de emisores del certificado debe coincidir con uno de los nombres distinguidos (DN) enviado por el servidor durante el protocolo de enlace TLS.

Cambie el modo en que se seleccionan los certificados, usando alguno de estos métodos:

- En la línea de comandos de Receiver, especifique la opción AM_CERTIFICATESELECTIONMODE={ Prompt | SmartCardDefault | LatestExpiry }.
  La opción predeterminada es "Prompt" (Preguntar). Para SmartCardDefault (predeterminado de la tarjeta inteligente) o LatestExpiry (fecha de caducidad más lejana), si hay varios certificados que cumplen esos criterios, Receiver pide al usuario que elija uno.

- Agregue el siguiente valor a la clave de Registro en HKCU o HKLM\Software\[Wow6432Node\]Citrix\AuthManager:
  CertificateSelectionMode={ Prompt | SmartCardDefault | LatestExpiry }.

Los valores definidos en HKCU tienen preferencia sobre los valores definidos en HKLM para facilitar al usuario la selección de certificado.

De manera predeterminada, los diálogos de PIN que se presentan a los usuarios provienen de Receiver en lugar de venir del proveedor CSP (Cryptographic Service Provider) de la tarjeta inteligente. Receiver pide a los usuarios que introduzcan un PIN cuando es necesario, y luego pasa el PIN al proveedor CSP de la tarjeta inteligente. Si el sitio o la tarjeta inteligente tiene unos requisitos de seguridad más estrictos como, por ejemplo, prohibir el almacenamiento del PIN en caché por proceso o por sesión, puede configurar Receiver para que use los componentes del CSP para gestionar las entradas de PIN, incluida la solicitud del PIN.

Cambie el modo en que se gestiona la entrada del PIN, usando alguno de estos métodos:

- En la línea de comandos de Receiver, especifique la opción AM_SMARTCARDPINENTRY=CSP.
- Agregue el siguiente valor a la clave de Registro HKLM\Software\[Wow6432Node\]Citrix\AuthManager: SmartCardPINEntry=CSP.

Para habilitar la comprobación de listas de revocación de certificados para mejorar las seguridad con Receiver

Dec 03, 2015

Cuando está habilitada la comprobación de la lista de revocación de certificados (CRL), Receiver verifica si el certificado del servidor se ha revocado. Al obligar a Receiver a realizar esta verificación, se puede mejorar la autenticación por cifrado del servidor, así como la seguridad general de las conexiones TLS entre los dispositivos de usuario y el servidor.

Se pueden habilitar varios niveles de verificación de revocación de certificados (CRL). Por ejemplo, se puede configurar Receiver para que verifique sólo la lista local de certificados, o bien que verifique las listas de certificados locales y de red. Además, se puede configurar la verificación de certificados para permitir que los usuarios inicien sesiones solo cuando se verifiquen todas las listas de revocación de certificados.

Si va a realizar este cambio en un equipo local, salga de Receiver si se está ejecutando. Compruebe que todos los componentes de Receiver, incluso la Central de conexiones, estén cerrados.

1. Como administrador, abra el Editor de directivas de grupo mediante la ejecución de gpedit.msc localmente desde el menú Inicio si va a aplicar directivas para un solo equipo, o bien, mediante la Consola de administración de directivas de grupo si va a aplicar directivas de dominio.
   Nota: Si ya importó la plantilla icaclient al Editor de directivas de grupo, puede omitir los pasos 2 a 5.
2. En el panel izquierdo del Editor de directivas de grupo, seleccione la carpeta Plantillas administrativas.
3. En el menú Acción, seleccione Agregar o quitar plantillas.
4. Seleccione Agregar y vaya a la carpeta Configuration de Receiver (normalmente C:\Archivos de programa\Citrix\ICA Client\Configuration) y seleccione icaclient.adm.
5. Seleccione Abrir para agregar la plantilla y luego, haga clic en Cerrar para regresar al Editor de directivas de grupo.
6. Desde el Editor de directivas de grupo, expanda Plantillas administrativas> Plantillas administrativas clásicas (ADM) > Citrix Components > Citrix Receiver > Network routing > TLS/SSL data encryption and server identification.
7. En el menú Acción, elija Propiedades y seleccione Habilitada.
8. En el menú desplegable CRL Verification, elija una de las opciones.
   - Inhabilitada No se lleva a cabo la verificación de revocación.
   - Only check locally stored CRLs. CRL que se instalaron o descargaron anteriormente y que se utilizan en la validación del certificado. Si se revoca el certificado, la conexión falla.
   - Require CRLs for connection. Se verifican los CRL locales y de los emisores de certificados pertinentes en la red. Si se revoca el certificado o no se encuentra, la conexión falla.
   - Retrieve CRLs from network. Se verifican los CRL de los emisores de certificados pertinentes. Si se revoca el certificado, la conexión falla.

   Si no configura un valor para CRL verification, se usará el valor predeterminado: Only check locally stored CRLs.

Protección de las comunicaciones de Receiver

Nov 19, 2015

Para proteger la comunicación entre la los sitios de XenDesktop o las comunidades de servidores XenApp y Receiver, se pueden integrar las conexiones de Receiver a través de tecnologías de seguridad como las siguientes:

- Citrix NetScaler Gateway o Access Gateway. Para obtener más información, consulte los temas de esta sección además de la documentación de NetScaler Gateway, Access Gateway y StoreFront.
  Nota: Citrix recomienda utilizar NetScaler Gateway para proteger las comunicaciones entre los servidores StoreFront y los dispositivos de los usuarios.
- Un firewall. Los firewall o servidores de seguridad de red pueden permitir o bloquear los paquetes basándose en la dirección y el puerto de destino. Si desea utilizar Receiver a través de un firewall que asigna la dirección IP de red interna del servidor a una dirección de Internet externa (es decir, traducción de direcciones de red, NAT), configure las direcciones externas.
- Configuración de confianza del servidor.
- Solamente para implementaciones de XenApp o la Interfaz Web; no se aplica a XenDesktop 7: un servidor proxy SOCKS o un servidor proxy seguro (también conocido como servidor proxy de seguridad o servidor proxy HTTPS). Se pueden utilizar servidores proxy para limitar el acceso hacia y desde la red, y para gestionar las conexiones entre Receiver y los servidores. Receiver respalda protocolos de proxy seguro y SOCKS.
- Para implementaciones de XenApp o Interfaz Web solamente; no se aplica a XenDesktop 7, XenDesktop 7.1, XenDesktop 7.5 o XenApp 7.5: Soluciones de Traspaso SSL con protocolos TLS (Transport Layer Security).
- Para XenApp 7.6 y XenDesktop 7.6, puede habilitar una conexión SSL directamente entre los usuarios y los VDA. (Consulte SSL para ver información sobre cómo configurar SSL para XenApp 7.6 o XenDesktop 7.6).

Receiver es compatible con entornos en los que se utilizan las plantillas de seguridad de escritorio de Microsoft Specialized Security - Limited Functionality (SSLF). Estas plantillas se respaldan en las plataformas Microsoft Windows XP, Windows Vista y Windows 7. Consulte las guías de seguridad de Windows XP, Windows Vista y Windows 7 disponibles en http://technet.microsoft.com para obtener más información sobre las plantillas y su configuración.

Conexión con NetScaler Gateway

Nov 03, 2016

Para permitir que los usuarios remotos se conecten a través de NetScaler Gateway, configúrelo para que funcione con StoreFront.

- Para implementaciones de StoreFront: puede permitir conexiones de usuarios remotos o internos en StoreFront a través de NetScaler Gateway integrando NetScaler Gateway y StoreFront. Esta implementación permite que los usuarios se conecten a StoreFront para acceder a las aplicaciones y los escritorios virtuales. Los usuarios se conectan mediante Citrix Receiver.

Para obtener información sobre la configuración de estas conexiones, consulte Integración de NetScaler Gateway con XenMobile App Edition y los demás temas incluidos en ese nodo en la Documentación de productos Citrix. En los siguientes temas, se ofrece información sobre los parámetros que se requieren en Receiver para Windows:

- Configuración de perfiles y directivas de sesión para XenMobile App Edition
- Creación del perfil de sesión para Receiver para XenMobile App Edition
- Configuración de directivas personalizadas de acceso sin cliente para Receiver

Para permitir que los usuarios remotos se conecten mediante NetScaler Gateway a la implementación de la Interfaz Web, configure NetScaler Gateway para que funcione con la Interfaz Web, como se describe en Cómo dar acceso a aplicaciones publicadas y escritorios virtuales a través de la Interfaz Web y los temas secundarios correspondientes en la Documentación de productos Citrix.

Conexión con Access Gateway Enterprise Edition

Nov 03, 2016

Para permitir que los usuarios remotos se conecten mediante Access Gateway, configure Access Gateway para que funcione con StoreFront y AppController (un componente de CloudGateway).

- Para implementaciones de StoreFront: puede permitir conexiones de usuarios remotos o internos en StoreFront a través de Access Gateway integrando Access Gateway y StoreFront. Esta implementación permite que los usuarios se conecten a StoreFront para acceder a las aplicaciones y los escritorios virtuales. Los usuarios se conectan mediante Citrix Receiver.
- Para implementaciones de AppController: puede permitir conexiones de usuarios remotos con AppController integrando Access Gateway y AppController. Con esta implementación, los usuarios pueden conectarse a AppController para obtener aplicaciones Web y de software como servicio (SaaS), y pueden usar los servicios de ShareFile Enterprise con Receiver. Los usuarios se conectan mediante Receiver o mediante el Access Gateway Plug-in.

Para obtener información sobre la configuración de estas conexiones, consulte Integrating Access Gateway with CloudGateway y los demás temas incluidos en ese nodo en la Documentación de productos Citrix. En los siguientes temas, se ofrece información sobre los parámetros que se requieren en Receiver para Windows:

- Configuración de directivas de sesión y perfiles de CloudGateway
- Creación del perfil de sesión destinado a Receiver para CloudGateway Enterprise
- Creación del perfil de sesión destinado a Receiver para CloudGateway Express
- Configuración de directivas personalizadas de acceso sin cliente para Receiver

Para permitir que los usuarios remotos se conecten mediante Access Gateway a la implementación de la Interfaz Web, configure Access Gateway para que funcione con la Interfaz Web, como se describe en Configuring Access Gateway Enterprise Edition to Communicate with the Web Interface y los subtemas correspondientes en la Documentación de productos Citrix.

Conexión con Secure Gateway

Dec 03, 2015

Este tema solo se aplica a entornos donde se usa la Interfaz Web.

Es posible usar Secure Gateway en modo Normal o en modo Relay (Traspaso) para proporcionar un canal de comunicaciones seguro entre Receiver y el servidor. No es necesario configurar Receiver si se utiliza Secure Gateway en modo Normal y los usuarios se conectan a través de la Interfaz Web.

Receiver usa parámetros que se configuran de forma remota en el servidor que ejecuta la Interfaz Web para conectarse a los servidores que ejecutan Secure Gateway. Consulte los temas de la Interfaz Web para obtener información sobre la configuración de los parámetros del servidor proxy para Receiver.

Si se instala Secure Gateway Proxy en un servidor de una red segura, se puede utilizar Secure Gateway Proxy en modo Relay. Consulte los temas de Secure Gateway a fin de obtener más información sobre el modo Relay.

Si se utiliza el modo Relay, el servidor Secure Gateway funciona como un proxy y es necesario configurar Receiver para que use lo siguiente:

- El nombre de dominio completo (FQDN) del servidor Secure Gateway.
- El número de puerto del servidor Secure Gateway. Tenga en cuenta que el modo Relay no recibe respaldo en la versión 2.0 de Secure Gateway.

El nombre de dominio completo (FQDN) debe tener los siguientes tres componentes, consecutivamente:

- Host name
- Dominio intermedio
- Dominio superior

Por ejemplo: mi_equipo.mi_empresa.com es un nombre de dominio completo porque contiene el nombre de host (mi_equipo), un dominio intermedio (mi_empresa) y un dominio superior (com). Por lo general, la combinación de nombre de dominio intermedio y dominio superior (mi_empresa.com) se conoce como nombre de dominio.

Conexión a través de un firewall

Dec 03, 2015

Los firewall o servidores de seguridad de red pueden permitir o bloquear los paquetes basándose en la dirección y el puerto de destino. Si se utiliza un servidor de seguridad en el entorno, Receiver debe poder comunicarse a través del servidor de seguridad con el servidor Web y el servidor Citrix. El servidor de seguridad debe permitir el tráfico HTTP para la comunicación entre el dispositivo de usuario y el servidor Web (normalmente mediante un puerto HTTP 80 estándar o 443 si se usa un servidor Web seguro). Para las comunicaciones entre Receiver y el servidor Citrix, el servidor de seguridad debe permitir el tráfico ICA entrante en los puertos 1494 y 2598.

Si el servidor de seguridad se ha configurado para la traducción de direcciones de red (NAT), es posible usar la Interfaz Web para definir las asignaciones desde las direcciones internas hacia las direcciones externas y los puertos. Por ejemplo, si el servidor XenApp o XenDesktop no se ha configurado con una dirección alternativa, es posible configurar la Interfaz Web para proporcionar una dirección alternativa a Receiver. A continuación, Receiver se conecta con el servidor mediante la dirección externa y el número de puerto. Para obtener más información, consulte la documentación de la Interfaz Web.

Cumplimiento de relaciones de confianza

Dec 03, 2015

La configuración de confianza del servidor está diseñada para identificar y forzar relaciones de confianza en las conexiones de Receiver. La relación de confianza aumenta la sensación de seguridad de los administradores y usuarios de Receiver respecto a la integridad de la información en los dispositivos de usuario y evita el uso fraudulento o malintencionado de las conexiones de Receiver.

Cuando esta función está habilitada, los clientes pueden especificar los requisitos de confianza y determinar si confían en la conexión con el servidor. Por ejemplo, si Receiver se conecta a una dirección determinada (como, por ejemplo, https://*.citrix.com) con un tipo de conexión específico (por ejemplo, TLS) se redirige a una zona de confianza en el servidor.

Cuando se habilita la configuración de servidor de confianza, los servidores conectados deben residir en la zona de sitios de confianza de Windows. (Para ver instrucciones detalladas sobre cómo agregar servidores a la zona de sitios de confianza de Windows, consulte la ayuda en pantalla de Internet Explorer).

Para habilitar las configuraciones de confianza del servidor

Si cambia esto en un equipo local, cierre todos los componentes de Receiver, incluso la Central de conexiones.

1. Como administrador, abra el Editor de directivas de grupo mediante la ejecución de gpedit.msc localmente desde el menú Inicio si va a aplicar directivas para un solo equipo, o bien, mediante la Consola de administración de directivas de grupo si va a aplicar directivas de dominio.
   Nota: Si ya importó la plantilla icaclient al Editor de directivas de grupo, puede omitir los pasos 2 a 5.
2. En el panel izquierdo del Editor de directivas de grupo, seleccione la carpeta Plantillas administrativas.
3. En el menú Acción, seleccione Agregar o quitar plantillas.
4. Seleccione Agregar y vaya a la carpeta Configuration de Receiver (normalmente C:\Archivos de programa\Citrix\ICA Client\Configuration) y seleccione icaclient.adm.
5. Seleccione Abrir para agregar la plantilla y luego, haga clic en Cerrar para regresar al Editor de directivas de grupo.
6. Expanda la carpeta Plantillas administrativas en el nodo Configuración del usuario.
7. Desde el Editor de directivas de grupo, expanda Plantillas administrativas> Plantillas administrativas clásicas (ADM) > Citrix Components > Citrix Receiver > Network routing > Configure trusted server configuration.
8. En el menú Acción, elija Propiedades y seleccione Habilitada.

Nivel de elevación y wfcrun32.exe

Dec 03, 2015

Cuando se habilita el control de cuentas de usuario (UAC) en los dispositivos que ejecutan Windows 8, Windows 7 o Windows Vista, sólo los procesos que se encuentren en el mismo nivel de integridad o elevación que wfcrun32.exe pueden iniciar las aplicaciones virtuales.

Ejemplo 1:

Cuando wfcrun32.exe se ejecuta como un usuario normal (no elevado), otros procesos como Receiver deben ejecutarse como usuario normal para poder iniciar aplicaciones a través de wfcrun32.

Ejemplo 2:

Cuando wfcrun32.exe se ejecuta en modo elevado, otros procesos como Receiver, la Central de conexiones y aplicaciones de terceros que usan el objeto Cliente ICA y que se están ejecutando en modo no elevado no se pueden comunicar con wfcrun32.exe.

Conexión de Receiver a través de un servidor proxy

Dec 03, 2015

Este tema solo se aplica a entornos donde se usa la Interfaz Web.

Los servidores proxy se usan para limitar el acceso hacia y desde la red, y para administrar conexiones entre los dispositivos Receiver y los servidores. Receiver respalda protocolos de proxy seguro y SOCKS.

En la comunicación con la comunidad de servidores, Receiver utiliza los parámetros de servidor proxy configurados de forma remota en el servidor que ejecuta Receiver para Web o la Interfaz Web. Para obtener más información sobre la configuración de servidores proxy, consulte la documentación de StoreFront o de la Interfaz Web.

En la comunicación con el servidor Web, Receiver utiliza los parámetros de servidor proxy configurados a través de la configuración de Internet del explorador Web predeterminado en el dispositivo de usuario. Se deben configurar los parámetros de Internet del explorador Web predeterminado en el dispositivo de usuario según corresponda.

Conexión con el Traspaso SSL (Secure Sockets Layer Relay)

Dec 03, 2015

Este tema no es aplicable a XenDesktop 7, XenDesktop 7.1, XenDesktop 7.5 o XenApp 7.5.

Puede integrar Receiver con los servicios de Traspaso SSL (Secure Sockets Layer Relay). Receiver respalda los protocolos TLS. Receiver 4.2 para Windows solo respalda TLS 1.0.

- TLS (Transport Layer Security) es la versión estándar más reciente del protocolo SSL. La organización Internet Engineering Taskforce (IETF) le cambió el nombre a TLS al asumir la responsabilidad del desarrollo de SSL como un estándar abierto. TLS protege las comunicaciones de datos mediante la autenticación del servidor, el cifrado del flujo de datos y la comprobación de la integridad de los mensajes. Algunas organizaciones, entre las que se encuentran organizaciones del gobierno de los EE. UU., requieren el uso de TLS para las comunicaciones de datos seguras. Estas organizaciones también pueden exigir el uso de cifrado validado, como FIPS 140 (Estándar federal de procesamiento de información). FIPS 140 es un estándar para cifrado.

De forma predeterminada, el Traspaso SSL Citrix utiliza el puerto TCP 443 en el servidor XenApp para las comunicaciones protegidas con TLS. Cuando el Traspaso SSL recibe una conexión TLS, descifra los datos antes de redirigirlos al servidor o al servicio Citrix XML Service (si el usuario ha seleccionado la exploración TLS+HTTPS).

Si configuró el Traspaso SSL en un puerto de escucha que no sea 443, debe especificar en el plug-in el puerto de escucha no estándar.

Puede utilizar el Traspaso SSL Citrix para proteger las comunicaciones:

- Entre los clientes con seguridad TLS habilitada y un servidor. Las conexiones que utilizan el cifrado TLS están marcadas con un icono de candado en la Central de conexiones de Citrix.
- Con un servidor que ejecuta la Interfaz Web, entre el equipo que ejecuta el servidor XenApp y el servidor Web.

Para obtener más información sobre la configuración del Traspaso SSL para proteger la instalación, consulte la documentación de XenApp.

Además de los requisitos del sistema, debe asegurarse de que:

- El dispositivo de usuario admita el cifrado de 128 bits
- El dispositivo de usuario disponga de un certificado raíz instalado que pueda verificar la firma de la entidad emisora de certificados con el certificado del servidor
- Receiver conoce el número de puerto de escucha TCP utilizado por el servicio de Traspaso SSL en la comunidad de servidores.
- Se han aplicado todos los Service Packs y actualizaciones recomendadas por Microsoft.

Si utiliza Internet Explorer y no conoce el nivel de cifrado del sistema, vaya al sitio Web de Microsoft en http://www.microsoft.com para instalar un Service Pack que proporcione el cifrado de 128 bits.

Importante: Receiver admite longitudes de claves de certificado de hasta 4096 bits. Asegúrese de que las longitudes de bits de los certificados intermedios y del certificado raíz de la entidad emisora de certificados y de los certificados del servidor

no excedan la longitud en bits que admite Receiver, dado que podría fallar la conexión.

Si cambia esto en un equipo local, cierre todos los componentes de Receiver, incluso la Central de conexiones.

1. Como administrador, abra el Editor de directivas de grupo mediante la ejecución de gpedit.msc localmente desde el menú Inicio si va a aplicar directivas para un solo equipo, o bien, mediante la Consola de administración de directivas de grupo si va a aplicar directivas de dominio.
   Nota: Si ya importó la plantilla icaclient al Editor de directivas de grupo, puede omitir los pasos 2 a 5.
2. En el panel izquierdo del Editor de directivas de grupo, seleccione la carpeta Plantillas administrativas.
3. En el menú Acción, seleccione Agregar o quitar plantillas.
4. Seleccione Agregar y vaya a la carpeta Configuration del plug-in (normalmente C:\Archivos de programa\Citrix\ICA Client\Configuration) y seleccione icaclient.adm.
5. Seleccione Abrir para agregar la plantilla y luego, haga clic en Cerrar para regresar al Editor de directivas de grupo.
6. Desde el Editor de directivas de grupo, expanda Plantillas administrativas> Plantillas administrativas clásicas (ADM) > Citrix Components > Citrix Receiver > Network routing > TLS/SSL data encryption and server identification.
7. En el menú Acción, elija Propiedades, seleccione Habilitada y, a continuación, escriba un número de puerto nuevo en el cuadro de texto Allowed SSL servers con el siguiente formato:

servidor:número de puerto de traspaso SSL

donde número de puerto de traspaso SSL es el número del puerto de escucha. Puede utilizar un comodín para especificar varios servidores. Por ejemplo, *.Test.com:número de puerto de traspaso SSL hace coincidir todas las conexiones Test.com a través del puerto especificado.

Si cambia esto en un equipo local, cierre todos los componentes de Receiver, incluso la Central de conexiones.

1. Como administrador, abra el Editor de directivas de grupo mediante la ejecución de gpedit.msc localmente desde el menú Inicio si va a aplicar directivas para un solo equipo, o bien, mediante la Consola de administración de directivas de grupo si va a aplicar directivas de dominio.
   Nota: Si ya agregó la plantilla icaclient al Editor de directivas de grupo, puede omitir los pasos 2 a 5.
2. En el panel izquierdo del Editor de directivas de grupo, seleccione la carpeta Plantillas administrativas.
3. En el menú Acción, seleccione Agregar o quitar plantillas.
4. Seleccione Agregar y vaya a la carpeta Configuration de Receiver (normalmente C:\Archivos de programa\Citrix\ICA Client\Configuration) y seleccione icaclient.adm.
5. Seleccione Abrir para agregar la plantilla y luego, haga clic en Cerrar para regresar al Editor de directivas de grupo.
6. Desde el Editor de directivas de grupo, expanda Plantillas administrativas> Plantillas administrativas clásicas (ADM) > Citrix Components > Citrix Receiver > Network routing > TLS/SSL data encryption and server identification.
7. En el menú Acción, elija Propiedades, seleccione Habilitada y, a continuación, escriba una lista de servidores de confianza separada con comas y el número de puerto nuevo en el cuadro de texto Allowed SSL servers con el siguiente formato:
   nombre_de_servidor:número de puerto de traspaso SSL,nombre_de_servidor:número de puerto de traspaso SSL

   donde número de puerto de traspaso SSL es el número del puerto de escucha. Puede especificar una lista de servidores SSL de confianza separados por comas similar a este ejemplo:
   csghq.Test.com:443,fred.Test.com:443,csghq.Test.com:444
   que se traduce a lo siguiente en el archivo appsrv.ini:
   [Word]

SSLProxyHost=csghq.Test.com:443

[Excel]

SSLProxyHost=csghq.Test.com:444

[Notepad]

SSLProxyHost=fred.Test.com:443

Configuración y habilitación de Receiver para usar TLS

Dec 03, 2015

Este tema no es aplicable a XenDesktop 7, XenDesktop 7.1, XenDesktop 7.5 o XenApp 7.5.

Para forzar la conexión de Receiver con TLS, se debe especificar TLS en el servidor Secure Gateway o en el servicio Traspaso SSL. Para obtener más información, consulte los temas de la documentación de Secure Gateway o del servicio Traspaso de SSL.

Además, asegúrese de que el dispositivo de usuario cumple todos los requisitos del sistema.

Para usar el cifrado TLS para todas las comunicaciones de Receiver, configure el dispositivo de usuario, Receiver, y el servidor que ejecuta la Interfaz Web (en caso de que use la Interfaz Web). Para obtener más información sobre cómo proteger las comunicaciones con StoreFront, consulte los temas de "Seguridad" en la documentación de StoreFront.

Si se desea usar TLS para proteger la seguridad de las comunicaciones entre las instancias de Receiver habilitadas con TLS y la comunidad de servidores, se necesita un certificado raíz en el dispositivo de usuario que pueda verificar la firma de la entidad de certificación en el certificado del servidor.

Receiver respalda entidades emisoras de certificados compatibles con Windows. Los certificados raíz para estas entidades se instalan con Windows y se administran a través de las utilidades de Windows. Estos certificados son los mismos que utiliza Microsoft Internet Explorer.

Si utiliza su propia entidad emisora de certificados, debe obtener un certificado raíz de esa entidad emisora de certificados e instalarlo en cada dispositivo de usuario. Microsoft Internet Explorer y Receiver utilizarán este certificado.

Puede instalar el certificado raíz a través de otros métodos de administración y distribución, como:

- Con el administrador de perfiles y el asistente de configuración del Kit de administración de Internet Explorer (IEAK) de Microsoft.
- Con herramientas de distribución de terceros.

Asegúrese de que los certificados instalados por Windows cumplen los requisitos de seguridad de su organización; o bien, utilice los certificados emitidos por la entidad emisora de certificados de la organización.

1. Para usar TLS con el fin de cifrar los datos de enumeración e inicio de aplicaciones enviados entre Receiver y el servidor que ejecuta la Interfaz Web, configure los parámetros apropiados mediante la Interfaz Web. Debe incluir el nombre de equipo del servidor XenApp donde está el certificado SSL.
2. Para usar una conexión HTTP segura (HTTPS) para cifrar la información de configuración que se envía entre Receiver y el servidor que ejecuta la Interfaz Web, introduzca la dirección URL del servidor con el formato https://nombre_servidor. En el área de notificación de Windows, haga clic con el botón secundario en el icono de Receiver y seleccione Preferencias.
3. Haga clic con el botón secundario en la entrada Online Plug-in de Estado del plug-in y elija Cambiar servidor.

Si cambia esto en un equipo local, cierre todos los componentes de Receiver, incluso la Central de conexiones.

1. Como administrador, abra el Editor de directivas de grupo mediante la ejecución de gpedit.msc localmente desde el menú Inicio si va a aplicar esto en un solo equipo, o bien, mediante la Consola de administración de directivas de grupo si va a usar Active Directory.
   Nota: Si ya importó la plantilla icaclient al Editor de directivas de grupo, puede omitir los pasos 2 a 5.
2. En el panel izquierdo del Editor de directivas de grupo, seleccione la carpeta Plantillas administrativas.
3. En el menú Acción, seleccione Agregar o quitar plantillas.
4. Seleccione Agregar y vaya a la carpeta Configuration de Receiver (normalmente C:\Archivos de programa\Citrix\ICA Client\Configuration) y seleccione icaclient.adm.
5. Seleccione Abrir para agregar la plantilla y luego, haga clic en Cerrar para regresar al Editor de directivas de grupo.
6. Desde el Editor de directivas de grupo, expanda Plantillas administrativas> Plantillas administrativas clásicas (ADM) > Citrix Components > Citrix Receiver > Network routing > TLS/SSL data encryption and server identification.
7. En el menú Acción, elija Propiedades, seleccione Habilitada y luego, elija la configuración TLS en los menús desplegables.
   - Para habilitar TLS, configure la versión de TLS a TLS o Detect all. Si selecciona Detect all, Receiver intenta conectar usando el cifrado TLS.
   - Configure el conjunto de cifrado SSL (SSL ciphersuite) con Detect version para que Receiver pueda negociar un conjunto de cifrado gubernamental y comercial adecuado. Puede restringir el conjunto de cifrado, ya sea a uno gubernamental o a uno comercial.
   - Configure la verificación CRL (CRL verification) con el valor Require CRLs for connection que requiere que Receiver intente obtener listas de revocación de certificados (CRL) de los emisores de certificado relevantes.

Si cambia esto en un equipo local, cierre todos los componentes de Receiver, incluso la Central de conexiones.

Para cumplir con los requisitos de seguridad FIPS 140, utilice la plantilla de directivas de grupo a fin de configurar los parámetros o incluya los parámetros en el archivo Default.ica en el servidor donde se ejecuta la Interfaz Web. Para obtener más información sobre el archivo Default.ica, consulte la información sobre la Interfaz Web.

1. Como administrador, abra el Editor de directivas de grupo mediante la ejecución de gpedit.msc localmente desde el menú Inicio si va a aplicar directivas para un solo equipo, o bien, mediante la Consola de administración de directivas de grupo si va a aplicar directivas de dominio.
   Nota: Si ya importó la plantilla icaclient al Editor de directivas de grupo, puede omitir los pasos 3 a 5.
2. En el panel izquierdo del Editor de directivas de grupo, seleccione la carpeta Plantillas administrativas.
3. En el menú Acción, seleccione Agregar o quitar plantillas.
4. Seleccione Agregar y vaya a la carpeta Configuration de Receiver (normalmente C:\Archivos de programa\Citrix\ICA Client\Configuration) y seleccione icaclient.adm.
5. Seleccione Abrir para agregar la plantilla y luego, haga clic en Cerrar para regresar al Editor de directivas de grupo.
6. Desde el Editor de directivas de grupo, expanda Plantillas administrativas> Plantillas administrativas clásicas (ADM) > Citrix Components > Citrix Receiver > Network routing > TLS/SSL data encryption and server identification.
7. En el menú Acción, elija Propiedades, seleccione Habilitada y del menú elija la configuración correcta.
   - Para habilitar TLS, configure la versión de TLS como TLS o Detect all. Si selecciona Detect all, Receiver intenta conectar usando el cifrado TLS.
   - Configure SSL ciphersuite con el valor Government.
   - Configure CRL verification con el valor Require CRLs for connection.

Al utilizar la Interfaz Web, especifique el nombre de equipo del servidor que aloja el certificado SSL. Consulte la información

sobre la Interfaz Web para obtener más detalles sobre cómo usar TLS para proteger la seguridad de las comunicaciones entre Receiver y el servidor Web.

1. En el menú Configuración, seleccione Configuración del servidor.
2. Elija Usar SSL/TLS para las comunicaciones entre los clientes y el servidor Web.
3. Guarde los cambios.

La elección de SSL/TLS hace que las direcciones URL pasen a usar el protocolo HTTPS.

Es posible configurar el servidor XenApp para que utilice TLS a fin de proteger las comunicaciones entre Receiver y el servidor.

1. En la consola de administración de Citrix para el servidor XenApp, abra el cuadro de diálogo Propiedades para la aplicación que desea proteger.
2. Seleccione Avanzado > Opciones del cliente y asegúrese de seleccionar Habilitar SSL y TLS.
3. Repita estos pasos para cada aplicación que desee proteger.

Al utilizar la Interfaz Web, especifique el nombre de equipo del servidor que aloja el certificado SSL. Consulte la información sobre la Interfaz Web para obtener más detalles sobre cómo usar TLS para proteger la seguridad de las comunicaciones entre Receiver y el servidor Web.

Es posible configurar Receiver para que use TLS con el fin de proteger la seguridad de las comunicaciones entre Receiver y el servidor que ejecuta la Interfaz Web.

En este procedimiento se presupone que existe un certificado raíz válido instalado en el dispositivo de usuario. Para obtener más información, consulte Instalación de certificados raíz en los dispositivos de usuario.

1. En el área de notificación de Windows, haga clic con el botón secundario en el icono de Receiver y seleccione Preferencias.
2. Haga clic con el botón secundario en la entrada Online Plug-in de Estado del plug-in y elija Cambiar servidor.
3. La pantalla Cambiar servidor muestra la dirección URL configurada. Introduzca la dirección URL del servidor en el cuadro de texto siguiendo el formato https://nombre_de_servidor para cifrar los datos de configuración mediante TLS.
4. Haga clic en Actualizar para aplicar los cambios.
5. Habilite TLS en el explorador Web del dispositivo del usuario. Para obtener más información, consulte la Ayuda en línea del explorador.

Protección ante el inicio de aplicaciones y escritorios desde servidores que no son de confianza con ICA File Signing

Dec 03, 2015

Este tema solo es aplicable a implementaciones con Interfaz Web que usan Plantillas administrativas.

La función ICA File Signing (firma de archivos ICA) permite proteger a los usuarios ante inicios de escritorios y aplicaciones no autorizados. Citrix Receiver verifica si el inicio de la aplicación o del escritorio fue generado desde una fuente de confianza, basándose en una directiva de administración, y protege al usuario frente a inicios originados en servidores que no son de confianza. Esta directiva de seguridad de Receiver para la verificación de firmas de inicio de aplicaciones o escritorios se puede configurar mediante objetos de directiva de grupo, StoreFront o Citrix Merchandising Server. La función ICA File Signing no está habilitada de forma predeterminada. Para obtener más información sobre cómo habilitar ICA File Signing para StoreFront, consulte la documentación de StoreFront.

En los entornos con Interfaz Web, la Interfaz Web habilita y configura los inicios de escritorios y aplicaciones para incluir una firma durante el proceso de inicio mediante el servicio Citrix ICA File Signing. Este servicio permite firmar los archivos ICA con un certificado del almacén de certificados personal del equipo.

Citrix Merchandising Server con Receiver permite configurar e iniciar la verificación de firmas mediante el asistente de la consola de administración Citrix Merchandising Server Administrator Console > Deliveries para agregar sellos de certificados de confianza.

Para usar objetos de directiva de grupo para habilitar y configurar la verificación de firmas de inicio de aplicaciones o escritorios, siga este procedimiento:

1. Como administrador, abra el Editor de directivas de grupo mediante la ejecución de gpedit.msc localmente desde el menú Inicio si va a aplicar directivas para un solo equipo, o bien, mediante la Consola de administración de directivas de grupo si va a aplicar directivas de dominio.
   Nota: Si ya importó la plantilla ica-file-signing.adm al Editor de directivas de grupo, puede omitir los pasos 2 a 5.
2. En el panel izquierdo del Editor de directivas de grupo, seleccione la carpeta Plantillas administrativas.
3. En el menú Acción, seleccione Agregar o quitar plantillas.
4. Seleccione Agregar y vaya a la carpeta de configuración de Receiver (normalmente C:\Archivos de programa\Citrix\ICA Client\Configuration) y seleccione ica-file-signing.adm.
5. Seleccione Abrir para agregar la plantilla y luego, haga clic en Cerrar para regresar al Editor de directivas de grupo.
6. En el Editor de directivas de grupo, vaya a Plantillas administrativas > Plantillas administrativas clásicas (ADM) > Citrix Components > Citrix Receiver y vaya a Enable ICA File Signing.
7. Si elige Habilitada, podrá agregar sellos de certificados con firma a la lista blanca de certificados de confianza, o bien quitar los sellos de certificados con firma de la lista blanca haciendo clic en Mostrar y luego use la ventana Mostrar contenido. Puede copiar y pegar los sellos de certificados con firma desde las propiedades de los certificados. Use el menú desplegable Directiva para seleccionar Permitir inicios con firma solamente (más seguro) o Preguntar al usuario en inicios sin firma (menos seguro).

Opción	Descripción
Permitir inicios	Permite inicios de escritorios o aplicaciones con firma solamente desde servidores de confianza.

Opción	Descripción
con firma solamente (más seguro)	Si un inicio de escritorio o aplicación no dispone de una firma válida, se mostrará al usuario un mensaje de advertencia de seguridad en Receiver. El usuario no podrá continuar y se bloqueará el inicio no autorizado.
Preguntar al usuario en inicios sin firma (menos seguro)	Pregunta al usuario cada vez que se realizan intentos de inicio de aplicación o escritorio sin firma o con una firma no válida. El usuario tiene la opción de continuar el inicio de la aplicación o cancelar el inicio (valor predeterminado).

Cuando se seleccione un certificado de firma digital, Citrix recomienda elegir a partir de la lista siguiente, en el orden siguiente:

1. Adquiera un certificado con firma de código o un certificado con firma SSL a partir de una entidad de certificados pública (AC).
2. Si su empresa dispone de una entidad de certificados privada, cree un certificado con firma de código o un certificado con firma SSL a través de la entidad de certificados privada.
3. Utilice un certificado SSL existente, como el certificado del servidor de la Interfaz Web.
4. Cree un certificado raíz nuevo y distribúyalo a los dispositivos de usuario mediante un objeto de directiva de grupo o una instalación manual.

Configuración de un explorador Web y un archivo ICA para habilitar Single Sign-on y administrar conexiones seguras a servidores de confianza

Dec 03, 2015

Este tema solo se aplica a entornos donde se usa la Interfaz Web.

Para usar Single Sign-on (SSO) y administrar conexiones seguras en servidores de confianza, agregue la dirección del sitio del servidor Citrix en la Intranet local o las zonas de Sitios de confianza en Herramientas > Opciones de Internet > Seguridad de Internet Explorer del dispositivo de usuario. La dirección puede incluir los formatos de comodines (*) admitidos por Internet Security Manager (ISM) o pueden ser específicos como protocolo ://URL[:puerto].

Se debe usar el mismo formato tanto en el archivo ICA como en las entradas de sitios. Por ejemplo, si especificó un nombre completo de dominio (FQDN) en el archivo ICA, deberá especificar un FQDN en la entrada de zonas de sitios. Las conexiones XenDesktop solo usan un formato de nombre de grupo de escritorio.

http[s]://10.2.3.4

http[s]://10.2.3.*

http[s]://nombre_host

http[s]://fqdn.ejemplo.com

http[s]://*.ejemplo.com

http[s]://nombre-empresa.*.ejemplo.com

http[s]://*.ejemplo.co.uk

escritorio://nombre-20grupo

ica[s]://servidorxa1

ica[s]://servidorxa1.ejemplo.com

Agregue la dirección exacta al sitio de la Interfaz Web en la zona de sitios.

Ejemplos de direcciones de sitios Web

https://mi.empresa.com

http://10.20.30.40

http://servidor-host:8080

https://traspaso-SSL:444

Agregue la dirección con el formato escritorio://Nombre de grupo de escritorio. Si el nombre del grupo contiene espacios, sustituya cada espacio con -20.

Use uno de los formatos siguientes en el archivo ICA para la dirección del sitio del servidor Citrix. Use el mismo formato para agregarlo a las zonas Intranet local o Sitios de confianza en Herramientas > Opciones de Internet > Seguridad de Internet Explorer del dispositivo de usuario.

Ejemplo de entrada HttpBrowserAddress en archivo ICA

HttpBrowserAddress=XMLBroker.ServidorXenapp.ejemplo.com:8080

Ejemplos de entradas de dirección de servidor XenApp en archivo ICA

Si el archivo ICA contiene solo el campo **Dirección** del servidor XenApp, use uno de los formatos de entrada siguientes:

icas://10.20.30.40:1494

icas://mi.servidor-xenapp.empresa.com

ica://10.20.30.40

Configuración de los permisos de los recursos del cliente

Dec 03, 2015

Este tema solo se aplica a entornos donde se usa la Interfaz Web.

Puede configurar los permisos de recursos del cliente utilizando áreas para sitios restringidos y de confianza mediante:

- La adición del sitio de la Interfaz Web a la lista de sitios de confianza.
- La modificación de los parámetros nuevos del Registro

Nota: Debido a las mejoras hechas en Receiver, el procedimiento .ini disponible en las versiones anteriores del plug-in/Receiver se ha reemplazado con estos procedimientos.
Precaución: Si edita el Registro de forma incorrecta podrían generarse problemas graves que pueden hacer que sea necesario instalar nuevamente el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Asegúrese de hacer una copia de seguridad del registro antes de modificarlo.

Para agregar el sitio de la Interfaz Web a la lista de sitios de confianza

1. En el menú Herramientas de Internet Explorer, seleccione Opciones de Internet > Seguridad.
2. Seleccione el icono Sitios de confianza y haga clic en el botón Sitios.
3. En el campo de texto Agregar este sitio Web a la zona de, escriba la URL del sitio de la Interfaz Web y haga clic en Agregar.
4. Descargue los parámetros de Registro desde http://support.citrix.com/article/CTX133565 y haga los cambios necesarios en el Registro. Use SsonRegUpx86.reg para los dispositivos de usuario de Win32 y SsonRegUpx64.reg para los dispositivos de usuario de Win64.
5. Cierre la sesión y luego inicie una sesión nuevamente en el dispositivo de usuario.

Para cambiar los permisos de los recursos del cliente en el Registro

1. Descargue los parámetros de Registro desde http://support.citrix.com/article/CTX133565 e importe los parámetros en cada uno de los dispositivos de usuario. Use SsonRegUpx86.reg para los dispositivos de usuario de Win32 y SsonRegUpx64.reg para los dispositivos de usuario de Win64.
2. En el editor del Registro, vaya a HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Client Selective Trust y en las áreas apropiadas, cambie el valor predeterminado a los valores de acceso requeridos para cualquiera de los recursos siguientes:

Clave de recurso	Recurso
FileSecurityPermission	Unidades del cliente
MicrophoneAndWebcamSecurityPermission	Micrófonos y cámaras Web
ScannerAndDigitalCameraSecurityPermission	USB y otros dispositivos

Valor	Descripción
0	Sin acceso
1	Acceso de solo lectura
2	Acceso completo
3	Solicitar acceso al usuario

Receiver Desktop Lock

Nov 19, 2015

Puede usar Receiver Desktop Lock cuando los usuarios no necesiten interactuar con el escritorio local. Los usuarios pueden seguir usando Desktop Viewer (si está habilitado), pero solo verán el conjunto de opciones que sean estrictamente necesarias en la barra de herramientas: Ctrl+Alt+Supr, Preferencias, Dispositivos y Desconectar.

Receiver Desktop Lock funciona en máquinas unidas a dominios, que están habilitadas para el inicio de sesión único o SSON (Single Sign-on) y tienen un almacén configurado. No respalda sitios de PNA. Las versiones anteriores de Desktop Lock no reciben respaldo después de actualizar a Receiver 4.2.x para Windows.

Debe instalar Citrix Receiver para Windows con la opción /includeSSON . Debe configurar el almacén y Single Sign-On, ya sea usando el archivo .adm o con la opción de la línea de comandos.

A continuación, instale Receiver Desktop Lock como administrador usando el archivo CitrixReceiverDesktopLock.MSI disponible en citrix.com/downloads.

Requisitos del sistema para Citrix Receiver Desktop Lock

- Respaldado en Windows XP (Embedded Edition), Windows 7 (incluido Embedded Edition), Windows 7 Thin PC, Windows 8 y Windows 8.1.
- Se conecta a StoreFront solo a través de protocolos nativos.
- Puntos finales unidos a un dominio.
- Los dispositivos de usuario deben estar conectados a una red de área local (LAN) o a una red de área extensa (WAN).

Nota: El respaldo para Windows XP finalizó el 8 de abril de 2014, fecha en que Microsoft puso fin al periodo extendido de respaldo para Windows XP.

Acceso a aplicaciones locales

Precaución: Si se habilita el acceso a aplicaciones locales se puede permitir el acceso al escritorio local, a menos que se haya aplicado un bloqueo completo mediante una plantilla de objeto de directiva de grupo o una directiva similar. Consulte Configuración del acceso a aplicaciones locales y la redirección de URL en XenApp y XenDesktop para obtener más información.

Cómo trabajar con Receiver Desktop Lock

- Receiver Desktop Lock puede usarse con las siguientes características de Receiver para Windows:
  - 3Dpro, Flash, USB, HDX Insight, plug-in de Microsoft Lync 2013 y acceso a aplicaciones locales
  - Solo autenticación de dominio, autenticación de dos factores o autenticación con tarjeta inteligente.
- Al desconectar la sesión de Receiver Desktop Lock se cierra la sesión del dispositivo final.
- La redirección de Flash está inhabilitada en Windows 8 y versiones posteriores. La redirección de Flash está habilitada en Windows 7.
- Desktop Viewer está optimizado para Receiver Desktop Lock y no incluye las propiedades Inicio, Restaurar, Maximizar ni Pantalla.
- Ctrl+Alt+Supr está disponible en la barra de herramientas de Desktop Viewer.
- La mayoría de las teclas de acceso directo de Windows se pasan a la sesión remota, excepto Windows+L Para ver más información, consulte Paso de las teclas de acceso directo de Windows a la sesión remota.
- Ctrl+F1 activa Ctrl+Alt+Supr cuando se inhabilita la conexión o Desktop Viewer para conexiones de escritorio.

Para instalar Receiver Desktop Lock

Este procedimiento instala Receiver para Windows de forma que los escritorios virtuales se muestren mediante Receiver Desktop Lock. Para las implementaciones donde se usan tarjetas inteligentes, consulte Para configurar tarjetas inteligentes y usarlas con dispositivos que ejecutan Receiver Desktop Lock.

1. Inicie sesión con una cuenta de administrador local.
2. En el símbolo del sistema, ejecute el siguiente comando (ubicado en los medios de instalación, en la carpeta Citrix Receiver y Plug-ins > Windows > Receiver).
   Para Receiver 4.2 para Windows:
   CitrixReceiver.exe /includeSSON STORE0="*DesktopStore*;https://*my.storefront.server*/Citrix/MyStore/discovery;on;*Desktop Store*"
   Para ver detalles del comando, consulte la documentación de instalación de Receiver para Windows en Configuración e instalación de Receiver para Windows mediante parámetros de línea de comandos.
3. En la misma carpeta de los medios de instalación, haga doble clic en CitrixReceiverDesktopLock.msi. Se abrirá el asistente de Desktop Lock. Siga las indicaciones.
4. Cuando se complete la instalación, reinicie el dispositivo de usuario. Si dispone de permisos para acceder a un escritorio e inicia sesión como un usuario de dominio, el dispositivo se muestra mediante Receiver Desktop Lock.

Para poder administrar el dispositivo de usuario una vez finalizada la instalación, la cuenta que se utilizó para instalar CitrixReceiverDesktopLock.msi se excluye del shell sustituto. Si, más adelante, esa cuenta se elimina, no podrá iniciar sesión ni administrar el dispositivo.

Para ejecutar una **instalación silenciosa** de Receiver Desktop Lock, use la siguiente línea de comandos: msiexec /i CitrixReceiverDesktopLock.msi /qn

Para configurar Receiver Desktop Lock

Otorgue acceso solamente a un escritorio virtual de Receiver Desktop Lock por usuario.

Mediante directivas de Active Directory, impida que los usuarios pongan a hibernar los escritorios virtuales.

Para configurar Receiver Desktop Lock, use la misma cuenta de administrador que utilizó para instalarlo.

- Compruebe que los archivos icaclient.adm y icaclient_usb.adm se han cargado en la directiva de grupo (las directivas aparecen en: Configuración del equipo o Configuración de usuario > Plantillas administrativas > Plantillas administrativas clásicas (ADM) > Componentes de Citrix). Los archivos ADM están ubicados en %ProgramFiles%\Citrix\ICA Client\Configuration\.
- Preferencias de USB. Cuando un usuario conecta un dispositivo USB, ese dispositivo se comunica automáticamente de forma remota con el escritorio virtual, por lo que no se requiere ninguna interacción por parte del usuario. El escritorio virtual es el que controla el dispositivo USB y lo muestra en la interfaz de usuario.
  - Habilite la regla de directivas USB.
  - En Citrix Receiver > Remoting client devices > Generic USB Remoting, habilite y configure las directivas Existing USB Devices y New USB Devices.
- Asignación de unidades. En Citrix Receiver > Remoting client devices, habilite y configure la directiva Client drive mapping.
- Micrófono. En Citrix Receiver > Remoting client devices, habilite y configure la directiva Client microphone.

Para configurar tarjetas inteligentes y usarlas con dispositivos que ejecutan Receiver Desktop Lock

1. Configure StoreFront.
   1. Configure XML Service para usar resolución de direcciones DNS para dar respaldo a Kerberos.
   2. Configure los sitios de StoreFront para el acceso mediante HTTPS, cree un certificado de servidor firmado por la entidad de certificación de su dominio y agregue un enlace HTTPS al sitio Web predeterminado.
   3. Compruebe que está habilitada la autenticación PassThrough con tarjeta inteligente (está habilitada de manera predeterminada).
   4. Habilite Kerberos.
   5. Habilite Kerberos y PassThrough con tarjeta inteligente.
   6. Habilite el Acceso anónimo en el sitio Web predeterminado de IIS y use la Autenticación de Windows integrada.
   7. Asegúrese de que el sitio Web predeterminado de IIS no requiera SSL e ignore los certificados de cliente.
2. Use la Consola de administración de directivas de grupo para configurar las directivas de equipo local en el dispositivo de usuario.

1. Importe la plantilla icaclient.adm desde %ProgramFiles%\Citrix\ICA Client\Configuration\.
2. Expanda Plantillas administrativas > Plantillas administrativas clásicas (ADM) > Citrix Components > Citrix Receiver > User authentication.
3. Habilite Smart card authentication.
4. Habilite Local user name and password.

3. Configure el dispositivo del usuario antes de instalar Receiver Desktop Lock.
    1. Agregue la dirección URL de Delivery Controller en la lista de Sitios de confianza de Internet Explorer en Windows.
    2. Agregue la URL del primer grupo de entrega a la lista de sitios de confianza de Internet Explorer en el formato escritorio://nombre-de-grupo-de-entrega.
    3. Permita a Internet Explorer que utilice el inicio de sesión automático en caso de sitios de confianza.

Cuando Receiver Desktop Lock está instalado en el dispositivo de usuario, se impone una directiva de extracción de tarjeta inteligente coherente. Por ejemplo, si la directiva de extracción de tarjetas inteligentes de Windows se establece en Forzar cierre de sesión para el escritorio, el usuario debe cerrar la sesión del dispositivo de usuario también, independientemente de cuál sea la directiva de extracción de tarjeta inteligente configurada en el equipo. Esto garantiza que el dispositivo de usuario no quede en un estado inconsistente. Esto se aplica solo a los dispositivos de usuario con Receiver Desktop Lock.

Para quitar Receiver Desktop Lock

Quite los dos componentes de la siguiente lista.

1. Inicie sesión con la misma cuenta de administrador local que se usó para instalar y configurar Receiver Desktop Lock.
2. Con la función de Windows para quitar o cambiar programas:
    - Quite Citrix Receiver Desktop Lock.
    - Quite Citrix Receiver.

Paso de las teclas de acceso directo de Windows a la sesión remota

La mayoría de las teclas de acceso directo de Windows se pasan a la sesión remota. Esta sección describe algunas de las más comunes.

Windows

- Win+D: Minimizar todas las ventanas en el escritorio.
- Alt+Tab: Cambiar la ventana activa.
- Ctrl+Alt+Supr: A través de Ctrl+F1 y la barra de herramientas de Desktop Viewer.
- Alt+Mayús+Tab
- Windows+Tab
- Windows+Mayús+Tab
- Windows+Todas las teclas de caracteres

Windows 8

- Win+C: Abrir accesos.
- Win+Q: Acceso Buscar.
- Win+H: Acceso Compartir.
- Win+K: Acceso Dispositivos.
- Win+I: Acceso Configuración.
- Win+Q: Buscar en Aplicaciones.
- Win+W: Buscar en Configuración.
- Win+F: Buscar en Archivos.

Aplicaciones de Windows 8

- Win+Z: Ir a opciones de la aplicación.

- Win+. : Acoplar aplicación a la izquierda.
- Win+Shift+. : Acoplar aplicación a la derecha.
- Ctrl+Tab: Navegar en ciclo por el historial de aplicaciones.
- Alt+F4: Cerrar una aplicación.

Escritorio

- Win+D: Abrir escritorio.
- Win+,: Vistazo de escritorio.
- Win+B: Volver al escritorio.

Otros

- Win+U: Abrir el Centro de accesibilidad.
- Ctrl+Esc: Pantalla Inicio.
- Win+Entrar: Abrir el Narrador de Windows.
- Win+X: Abrir el menú de configuración de herramientas del sistema.
- Win+ImprPant: Toma una captura de pantalla y la guarda en Imágenes.
- Win+Tab: Abre una lista de cambio de ventana.
- Win+T: Vista previa de ventanas abiertas en la barra de tareas.

Problemas resueltos de Citrix Receiver para Windows 4.x

Jan 20, 2017

Receiver para Windows 4.2.100

Comparado con: Citrix Receiver para Windows 4.2

Receiver para Windows 4.2.100 contiene todas las correcciones incluidas en Receiver para Windows 4.0, 4.0.1, 4.1, 4.1.2, 4.1.100, 4.1.200 y 4.2, además de las siguientes correcciones nuevas:

Teclado

- Cuando los usuarios reciben una solicitud para cambiar la contraseña, al presionar la combinación de teclas Ctrl + Alt + Fin en una sesión publicada de Receiver, es posible que la combinación de teclas no funcione.

  [En RcvrForWin4.2_14.2.100] [#LC0862]

Acceso a aplicaciones locales

- Cuando se usa la característica de acceso a aplicaciones locales "KEYWORDS:prefer="*patrón*"" con cualquier aplicación en XenApp 7.5 y StoreFront 2.5, Receiver puede tener problemas. Además, puede haber problemas durante la creación automática de accesos directos a aplicaciones preferidas mediante el "directorio de plantillas de preferencia".

  [En RcvrForWin4.2_14.2.100] [#LC2153]

Sesión/Conexión

- Al cambiar usuarios mediante la API de scripting de Fast Connect, el aviso sobre las credenciales no se cierra.

  [En RcvrForWin4.2_14.2.100] [#LC2299]

- Si los usuarios inician una sesión de escritorio en modo de pantalla completa y Desktop Viewer está inhabilitado, es posible que las barras de desplazamiento aparezcan al conectar un segundo monitor.

  Para habilitar la corrección, establezca la siguiente clave de Registro:

  - *En sistemas Windows de 32 bits*:
    HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client
    Nombre: ProcessWM_SETTINGCHANGE
    Tipo: DWORD

Valor: 1 (el valor predeterminado es 0). Esta corrección va dirigida únicamente a usuarios que inhabilitan la barra de CDViewer y ejecutan Desktop Viewer en modo de pantalla completa.

- *En sistemas Windows de 64 bits*:
  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client
  Nombre: ProcessWM_SETTINGCHANGE
  Tipo: DWORD
  Valor: 1 (el valor predeterminado es 0). Esta corrección va dirigida únicamente a usuarios que inhabilitan CDViewer Bar y ejecutan Desktop Viewer en modo de pantalla completa.

Las siguientes claves de Registro son optativas. De forma predeterminada, este valor es 0 y solo es necesario si la configuración predeterminada no soluciona el problema.

- *En sistemas Windows de 32 bits*:
  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client
  Nombre: MonitorLayoutUpdateDelay
  Tipo: DWORD
  Valor: de 0 a 4 (el valor predeterminado es 0)
- *En sistemas Windows de 64 bits*:
  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client
  Nombre: MonitorLayoutUpdateDelay
  Tipo: DWORD
  Valor: de 0 a 4 (el valor predeterminado es 0)

[En RcvrForWin4.2_14.2.100] [#LA5746]

- Esta mejora admite la "reconexión automática de clientes" en Receiver para Windows con XenApp 6.5 y sistemas operativos de servidor con la versión 7.x de VDA cuando los usuarios se conectan a NetScaler Gateway, y CloudBridge o HDX Insight están en la implementación.

  Nota: La fiabilidad de la sesión y la reconexión automática de clientes no funcionan si las directivas de multisecuencia y de puertos múltiples se habilitan en el servidor, y cuando se dan una de las siguientes condiciones o todas ellas:

  - La fiabilidad de la sesión está inhabilitada en NetScaler Gateway
  - Se produce una conmutación por error en el dispositivo NetScaler
  - CloudBridge se usa con NetScaler Gateway

  [En RcvrForWin4.2_14.2.100] [#LC1779]

- Al ejecutar Receiver con varios dispositivos USB conectados en el dispositivo del usuario, cuando se reinicia el dispositivo o se conecta un nuevo dispositivo USB, aparece el siguiente mensaje:

  "Energía del concentrador USB superada".

  [En RcvrForWin4.2_14.2.100] [#LC1904]

- Si los grupos de escritorios agrupados tienen varios escritorios configurados por usuario, solamente el primer escritorio puede iniciarse cuando se usa Receiver para Windows. Si el usuario hace clic en los iconos de los demás escritorios, es posible que el escritorio muestre el cuadro de diálogo "Conectando" y, a continuación, no consiga conectarse. La primera sesión de escritorio aparece en primer plano.

  [En RcvrForWin4.2_14.2.100] [#LC0780]

- Al importar el archivo de clave de Registro Client Selective Trust tal y como se describe en el artículo de Knowledge

Center CTX133565 y al configurar las zonas de confianza y de Intranet, si Desktop Viewer está habilitado en la Interfaz Web o en StoreFront, es posible que la clave del Registro no funcione. Si la URL de la Interfaz Web o de StoreFront está configurada como una zona de confianza en el explorador Web, aparece de forma incorrecta un mensaje acerca de la seguridad de los archivos al acceder al directorio de asignación de unidades del cliente (Client Drive Mapping, CDM).

[En RcvrForWin4.2_14.2.100] [#LC0904]

- Después de cerrar una sesión de escritorio, si el usuario intenta cerrar sesión en el cliente ligero de Windows XP Embedded, aparece el mensaje de error "Finalizar programa concentr.exe".

  [En RcvrForWin4.2_14.2.100] [#LC2556]

- La zona horaria no es correcta cuando los usuarios inician sesión con Receiver para Windows. Para que esta revisión hotfix funcione, deben cumplirse los siguientes requisitos:

  - La misma revisión hotfix de la actualización de la zona horaria de Microsoft debe estar instalada tanto en el dispositivo del usuario como en el servidor. Por ejemplo, si la revisión hotfix de Microsoft KB2998527 está instalada en el dispositivo del usuario, debe instalar esta revisión hotfix en el servidor.
  - Si el sistema operativo del servidor es Windows Server 2008 R2 Service Pack 1, la revisión hotfix de Microsoft KB2870165 debe estar instalada en el servidor.
  - La corrección #LC1061 debe instalarse en el servidor XenApp.

  [En RcvrForWin4.2_14.2.100] [#LC1392]

- Esta corrección habilita el respaldo de la API de scripting de Fast Connect sin que se integre con el Self-service Plug-in. Esto puede habilitarse mediante la directiva de grupo en **ADM** > **Citrix Components** > **Citrix Receiver** > **FastConnect API Support** > **Manage FastConnectAPI support** y, a continuación, al desmarcar la opción "Integrate Self Service plugin with FastConnect". También puede cambiar la clave de Registro "FastConnectUsingSSP" a "False" en HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\Dazzle.

  [En RcvrForWin4.2_14.2.100] [#LC2580]

- Cuando "SelfServiceMode" se establece en "False", se crean accesos directos del menú Inicio para las sesiones en segundo plano, como la aplicación de preinicio.

  [En RcvrForWin4.2_14.2.100] [#LC1760]

- Esta corrección va dirigida a los siguientes problemas:

  - Al iniciar una aplicación publicada integrada, es posible que esta aplicación se abra detrás de la barra de tareas de Windows.
  - Al mover la barra de tareas de Windows a otra ubicación, la sesión integrada no consigue cambiar de tamaño y es posible que la barra de tareas se solape con la aplicación integrada.

  Para habilitar esta corrección, también debe instalar la corrección #LC1342 del lado del servidor.

  [En RcvrForWin4.2_14.2.100] [#LC1645]

- Es posible que aparezca un mensaje de error al iniciar una sesión en Receiver para Windows 4.2 en un cliente ligero con Windows XP Embedded.

  [En RcvrForWin4.2_14.2.100] [#LC1929]

- Esta corrección habilita el respaldo de la API de scripting de Fast Connect en la instalación si establece

"FastConnectAPISupportEnabled=True". También puede habilitar este parámetro en el objeto de directiva de grupo "Enable FastConnect API Functionality", dentro de "Manage FastConnectAPI support".

[En RcvrForWin4.2_14.2.100] [#LC2131]

- Es posible que Receiver para Windows 4.2 deje de enviar paquetes de red debido a un interbloqueo en el programa. Como resultado, se pueden dar las siguientes situaciones:
  - Es posible que la sesión no se establezca.
  - Citrix HDX Engine puede dejar de responder si la resolución de pantalla del escritorio cambia.

  [En RcvrForWin4.2_14.2.100] [#LC2105]
- Esta mejora ofrece respaldo para las versiones 1.1 y 1.2 de TLS en la actualización acumulativa 1 de Receiver para Windows 4.2.

  [En RcvrForWin4.2_14.2.100] [#LC1931]
- El tiempo de retorno de sesión ICA del agente de EdgeSight puede ser elevado en sesiones aleatorias de la comunidad.

  [En RcvrForWin4.2_14.2.100] [#LC1725]
- Con esta mejora, el archivo "icaclient.adm" se modifica para mejorar la administración de los cambios de Fast Connect.

  [En RcvrForWin4.2_14.2.100] [#LC2575]
- Después de cambiar el tamaño de la sesión de Receiver al modo "Ajustar escala", el puntero y el teclado dejan de funcionar en la sesión.

  [En RcvrForWin4.2_14.2.100] [#LC2219]
- Este cambio mejora los registros de seguimiento de Citrix Diagnostic Facility (CDF) de la característica Fast Connect para que no informe de errores cuando no los hay.

  [En RcvrForWin4.2_14.2.100] [#LC2573]
- Después de la instalación de Receiver mediante la línea de comandos, un nuevo almacén se agrega automáticamente en el Self-service Plug-in al detener y reiniciar Receiver.

  El problema ocurre cuando la clave "Dazzle" en HKEY_CURRENT_USER\Software\Citrix tiene una subclave llamada "Properties" y "RegDeleteKey" no puede eliminar la clave del Registro que contiene las subclaves, y se crea un almacén de claves duplicado.

  [En RcvrForWin4.2_14.2.100] [#LC2154]
- Los accesos directos a las aplicaciones se quedan en la carpeta de accesos directos del escritorio o en el menú Inicio cuando los usuarios cierran sesión mediante las API de scripting de Fast Connect.

  [En RcvrForWin4.2_14.2.100] [#LC2590]
- Es posible que, al cerrar sesión mediante la API de scripting de Fast Connect, aparezcan varias ventanas de inicio de sesión para solicitudes sin autenticar.

  [En RcvrForWin4.2_14.2.100] [#LC2300]

- Al crear entradas de Registro relacionadas con Receiver antes de instalar el dispositivo Receiver, los usuarios estándar pueden instalar Receiver para Windows sin ningún error; sin embargo, es posible que las aplicaciones no se inicien.

  [En RcvrForWin4.2_14.2.100] [#LC0410]

- En la API de scripting de Fast Connect, es posible que el cambio de usuarios a una autenticación explícita no funcione.

  [En RcvrForWin4.2_14.2.100] [#LC2127]

- Esta mejora incluye la opción "Administración de accesos directos por aplicación". Mediante las propiedades de aplicación, puede crear accesos directos en el escritorio del usuario y en el menú Inicio para determinadas aplicaciones publicadas.

  Nota: La carpeta del menú Inicio de las propiedades de aplicación se respeta únicamente si los usuarios se conectan a la comunidad o a un grupo de entrega mediante la Interfaz Web en lugar de StoreFront.

  [En RcvrForWin4.2_14.2.100] [#LC1930]

- Cuando los usuarios cierran la sesión de Receiver mediante Fast Connect, la lista de suscripción de aplicaciones sigue apareciendo en el panel lateral.

  [En RcvrForWin4.2_14.2.100] [#LC2574]

- Si Receiver para Windows no está configurado con una cuenta, las aplicaciones no se pueden desconectar mediante el comando de desconexión de SelfService.

  [En RcvrForWin4.2_14.2.100] [#LC2128]

Excepciones del sistema

- Es posible que Receiver sufra una infracción de acceso y se cierre de forma inesperada. Cuando esto ocurre, los usuarios no pueden iniciar sesiones al hacer clic en los iconos de aplicación de la Interfaz Web.

  [En RcvrForWin4.2_14.2.100] [#LC0650]

- Al iniciar una aplicación publicada con una impresora local conectada a un dispositivo de usuario, es posible que Receiver para Windows se cierre de forma inesperada con el siguiente mensaje de error:

  "Citrix HDX Engine ha dejado de funcionar".

  [En RcvrForWin4.2_14.2.100] [#LC1170]

Experiencia de usuario

- Es posible que Receiver tarde mucho tiempo en crear accesos directos a las aplicaciones cuando los usuarios inician sesión en StoreFront o en la Interfaz Web.

  [En RcvrForWin4.2_14.2.100] [#LC2263]

- Con esta corrección, al leer la configuración de una sesión, la configuración de los objetos de directiva de grupo tiene mayor prioridad que el almacén principal.

  [En RcvrForWin4.2_14.2.100] [#LC2698]

Interfaz de usuario

- Después de la instalación de Receiver mediante la línea de comandos, el nombre y la descripción del almacén pasan a ser existentes. Si Receiver se reinicia, es posible que el nombre y la descripción del almacén cambien automáticamente a otro valor. No obstante, la URL sigue siendo la misma y la conexión funciona correctamente.

  El problema se produce porque, al procesar los sitios de Receiver, el nombre del almacén no se obtiene del Registro; en su lugar, se genera un nuevo nombre de almacén en función de la URL del almacén.

  [En RcvrForWin4.2_14.2.100] [#LC1231]

- Esta mejora suprime el aviso para quitar aplicaciones de la lista de aplicaciones, además de los accesos directos, si la aplicación ya no está publicada o está inhabilitada.

  [En RcvrForWin4.2_14.2.100] [#LC2157]

- El enlace "Más información" de Desktop Viewer va a un conjunto de archivos de ayuda distinto a lo que ven los usuarios cuando hacen clic en "Ayuda", en el menú de iconos de Receiver del área de navegación.

  [En RcvrForWin4.2_14.2.100] [#LC2066]

Receiver para Windows 4.2

Comparado con: Citrix Receiver para Windows 4.1.200

Receiver para Windows 4.2 contiene todas las correcciones incluidas en Receiver para Windows 4.0, 4.0.1, 4.1, 4.1.2, 4.1.100 y 4.1.200, además de las siguientes correcciones nuevas:

Redirección de contenido

- Al acceder a las direcciones URL de una aplicación publicada, es posible que la redirección de contenido de servidor a cliente no funcione, y que se pueda abrir un explorador Web en el servidor y que este no pueda abrirse en el cliente.

[#LC0150]

- En ocasiones, es posible que no se pueda acceder a un sitio Web que contenga una solicitud "HEAD" en el encabezado de la URL en lugar de una solicitud "GET" si el servidor Web no consigue aceptar la solicitud HEAD. Como resultado, la redirección de contenido de servidor a cliente no funciona.

  Para habilitar la corrección, cree la siguiente clave de Registro:

  HKEY_CURRENT_USER_\Software\Citrix\ICA Client\Engine
  Nombre: SpecificSites
  Tipo: REG_MULTI_SZ
  Valor: nombres de sitios Web (un sitio Web por línea)

  Nota: Se envía una solicitud GET en lugar de una solicitud HEAD a los sitios Web especificados en el valor. El nombre del sitio Web distingue entre mayúsculas y minúsculas, y permite el uso del carácter comodín "*". Por ejemplo, si se especifica "*.miempresa.com" en este valor del Registro, los usuarios podrán acceder tanto a www.miempresa.com como a asistencia.miempresa.com, los cuales son los sitios Web "específicos".

  [#LC0326]

- Esta corrección es una mejora de la corrección #LA0803. En los servidores con XenApp 6 Hotfix Rollup Pack 2 y XenApp 6.5 Hotfix Rollup Pack 3 instalados, al acceder a las direcciones URL personalizadas de una aplicación publicada, la redirección de contenido de servidor a cliente no funciona y se abre un explorador Web en el servidor en lugar de abrirse en el dispositivo del usuario.

  [#LC0428]

HDX MediaStream

- En un dispositivo de usuario con dos monitores, al reproducir un vídeo en el Reproductor de Windows Media en el primer monitor durante una sesión de Receiver, se abre una ventana negra adicional en el segundo monitor.

  [#LC0552]

- Al reproducir un vídeo en el Reproductor de Windows Media durante una sesión de Receiver, se abre una segunda ventana negra con el título "Citrix HDX Movie Window". El hecho de cerrar esta ventana secundaria no produce ningún efecto en el vídeo que se está reproduciendo.

  [#LC0818]

Redirección de Windows Media de HDX MediaStream

- Puede haber ruido estático al reproducir sonido mediante el Reproductor de Windows Media.

  [#LA2911]

HDX Plug and Play

- Durante las sesiones, es posible que, al quitar un dispositivo USB del dispositivo de punto final, Receiver para Windows deje de responder.

  [#LA4827]

- En ocasiones, los dispositivos USB no se liberan después de cerrar una sesión, y como consecuencia el dispositivo no se puede usar en la sesión local.

  [#LC0091]

Instalación, desinstalación y actualización

- Después de instalar Receiver con el modificador de línea de comandos /includeSSON, el proceso de SSONSVR.exe no llega a ejecutarse.

  [#LC0138]

- Si un administrador del sistema de Windows intenta desinstalar Receiver mediante el comando /uninstall de CitrixReceiver.exe, puede provocar que aparezca la solicitud del control de cuentas de usuario (UAC).

  [#LC0977]

Inicio de sesión/Autenticación

- El hecho de habilitar automáticamente la autenticación inteligente en la plantilla ADM del cliente provoca que el nombre y la contraseña de usuario local queden en estado "habilitado" en la directiva local aunque la directiva no se haya configurado anteriormente.

  [#LC0713]

- La autenticación PassThrough de dominio puede fallar de forma intermitente para la actualización acumulativa 3 de Citrix Receiver para Windows 3.4.

  [#LC0865]

Impresión

- Al configurar los parámetros de impresora local en Internet Explorer 8 para imprimir varias páginas por hoja, es posible que el parámetro no se respete; en su lugar, se imprime una página por hoja. El problema se produce en los casos en que el usuario se conecta desde un escritorio publicado de XenApp 6.5 a una instancia de Internet Explorer 8 publicada en un servidor XenApp 6.

  [#LA3379]

- Al hacer clic en "Vista previa en el cliente" mientras se usa el controlador de impresora universal XPS, aparece el siguiente mensaje de error en Internet Explorer:

  "Internet Explorer no puede mostrar la página web".

  [#LA5896]

- La creación automática de impresoras está limitada a 100 por sesión.

  [#LC0031]

- Esta mejora agrega el respaldo del seguimiento CDF al componente LPT del lado del cliente de asignación.

  [#LC0823]

Administración de servidores/comunidades

- Esta corrección soluciona un problema de memoria en un componente subordinado.

  [#LA5664]

- Cuando Receiver para Windows se conecta a NetScaler Gateway y, a continuación, pasa la conexión a StoreFront, solo la URL de servicio se incluye en la respuesta de StoreFront, y no las balizas. Cuando esto ocurre, los usuarios reciben un mensaje de error HTTP 403 y es posible que la detección automática no funcione.

  [#LC0481]

- Si el usuario inhabilita el parámetro "Concentrador raíz USB" y lo vuelve a habilitar desde el Administrador de dispositivos del dispositivo de usuario cuando este dispositivo se conecte a un VDA, la redirección de dispositivos USB no funciona.

  [#LC0541]

Sesión/Conexión

- Los inicios y los cierres de sesión en dispositivos cliente con Windows 7 y Receiver para Windows Enterprise Edition instalado pueden sufrir retrasos. El problema ocurre cuando un objeto de directiva de grupo aplica los scripts de inicio y cierre de sesión. Los scripts pueden causar una demora significativa.

  [#LA3811]

- Después de reanudar un dispositivo de punto final que estaba en modo de suspensión o hibernación cuando está conectado a una sesión de XenApp o XenDesktop a través de Receiver para Windows, las operaciones de copiar y pegar entre el dispositivo de punto final y la sesión de Citrix pueden fallar.

  [#LA3973]

- Con la multisecuencia habilitada, es posible que Receiver con Desktop Lock no consiga recuperarse de un protector de pantalla de VDA y no pueda volver a conectarse después de que el VDA se bloquee.

  [#LA4097]

- Al intentar abrir un archivo de Microsoft Word o Microsoft Excel 2003 desde una unidad de cliente asignada en la sesión con acceso de solo lectura, es posible que el archivo no se pueda abrir.

  [#LA4198]

- Con la directiva "Ocultar icono" habilitada, es posible que la ventana "Acerca de Citrix Receiver" aparezca automáticamente después de iniciar sesión en el dispositivo cliente.

  [#LA4513]

- Es posible que no se puedan iniciar sesiones mediante un controlador virtual personalizado.

  Para habilitar la corrección, debe crear la siguiente clave de Registro:

  - *En sistemas Windows de 32 bits*
    HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client
    Nombre: VdLoadUnLoadTimeOut

Tipo: REG_DWORD
Datos: Cualquier valor en segundos

- *En sistemas Windows de 64 bits*
  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432node\Citrix\ICA Client
  Nombre: VdLoadUnLoadTimeOut
  Tipo: REG_DWORD
  Datos: Cualquier valor en segundos

[#LA4540]

- En llamadas VoIP realizadas desde un VDA con PVS distribuido por streaming mediante HollyCRM con el plug-in Huawei OpenEye, es posible que un lado no escuche al otro después de dos horas o más.

  [#LA4809]

- Al presionar la tecla de Windows o al hacer clic en el botón Inicio para abrir el menú Inicio del lado del cliente con una ventana de sesión integrada en primer plano, hacer clic en el icono de la barra de tareas de una ventana local provoca que el enfoque permanezca en la ventana de sesión integrada en lugar de cambiar dicho enfoque a la ventana local.

  [#LA5089]

- Con el traspaso SSL habilitado, la fiabilidad de sesiones no consigue funcionar con aplicaciones configuradas para utilizar el cifrado.

  [#LA5476]

- Después de cambiar la contraseña en una sesión de escritorio publicado de XenApp, la autenticación PassThrough en aplicaciones publicadas desde la sesión de escritorio publicado falla, y los usuarios reciben un aviso para introducir su nombre de usuario y su contraseña.

  [#LA5587]

- Receiver falla al conectarse a StoreFront a través de NetScaler Gateway desde Windows Server 2012 R2.

  [#LC0084]

- En Receiver para Windows 4.1, se crea una segunda sesión de escritorio cuando los usuarios intentan volver a conectarse a una sesión desconectada al hacer clic en el icono de escritorio de la ventana del Self-service Plug-in.

  [#LC0182]

- Cleanup.exe puede cerrarse de forma inesperada al restablecer Receiver.

  [#LC0249]

- Durante el preinicio de sesión en entornos de XenApp que no estén en inglés, es posible que la barra de progreso de Citrix Receiver se vea y deje de responder con el siguiente mensaje de error:

  "Conexión establecida. Negociando capacidades...".

  [#LC0306]

- Escribir en instancias publicadas de Microsoft Outlook puede provocar que las sesiones se desconecten de forma aleatoria.

[#LC0323]

- Al intentar transferir archivos mediante dispositivos TWAIN con una aplicación de terceros, es posible que la aplicación se cierre de forma inesperada.

  [#LC0369]

- Cuando los usuarios se conectan a un VDA con Windows 7 a través de Receiver para Windows, si el usuario redirige SpeechMike mediante Desktop Viewer, es posible que la redirección falle al soltar el botón del micrófono.

  [#LC0510]

- Aunque la asociación de tipos de archivo esté configurada, los usuarios reciben un aviso para que elijan una aplicación con la que abrir el archivo correspondiente.

  [#LC0515]

- Los intentos de conexión a través de un servidor proxy mediante archivos PAC fallan.

  [#LC0529]

- Es posible que la actualización acumulativa 3 de Citrix Receiver para Windows 13.4 se cierre de forma inesperada para aplicaciones SAP publicadas con el siguiente mensaje de error:

  "Citrix HDX Engine ha dejado de funcionar".

  [#LC0712]

- El dispositivo de puertos COM redirigidos no funciona en sesiones de Receiver.

  [#LC0851]

- Si se aplica la corrección #LC0031, cuando los usuarios se desconectan o cierran la sesión, la sesión de Receiver deja de responder durante más de dos minutos cuando hay otras sesiones activas.

  [#LC0983]

Remedo

- Cuando los administradores intentan remedar una sesión, pueden provocar el inicio de una sesión de remedo con una pantalla en negro que no consiga redibujarse automáticamente. Este problema ocurre si la ventana que remeda y la ventana remedada tienen el mismo tamaño.

  [#LA2913]

Tarjetas inteligentes

- Es posible que Citrix Receiver para Windows no pueda encontrar un certificado de tarjeta inteligente válido y que aparezca el siguiente mensaje de error en el registro de depuración de Authentication Manager:

  "ERROR_WINHTTP_CLIENT_AUTH_CERT_NEEDED: Código de error desconocido '12044'".

  [#LC0783]

Excepciones del sistema

- Cuando un dispositivo cliente se reanuda desde el estado de hibernación, es posible que Receiver para Windows deje de responder.

  [#LA5023]

- Un problema con el proceso de CDViewer puede provocar una pantalla en negro y desencadenar una excepción no controlada de .Net.

  [#LC1038]

Experiencia de usuario

- En algunas configuraciones, es posible que se produzca un parpadeo del puntero en las sesiones de usuario.

  [#LA309]

- Con la función "Repetición local del texto" habilitada, es posible que, al escribir el símbolo de intercalación (^) en instancias publicadas de Internet Explorer, este parpadee o no sea visible en conexiones con una latencia elevada.

  [#LA4762]

- En ciertos casos, las aplicaciones se inician en segundo plano.

  [#LC0050]

- Si los usuarios abren varios libros de Excel y Excelhook está habilitado en el Registro, el icono de la barra de tareas de Excel desaparece al cerrar el último libro aunque la ventana de Excel esté abierta.

  [#LC0062]

- Cualquier usuario que no sea el que instaló Receiver recibe el aviso "Agregar cuenta" al iniciar Receiver por primera vez.

  [#LC0253]

- Tras reanudar la sesión desde "Apagar la pantalla", la sesión se presenta como una pantalla pequeña en la esquina superior izquierda del monitor.

  [#LC0319]

- Es posible que, al intentar mover la ventana de una aplicación publicada detrás de la barra local de tareas de Windows, no se pueda.

  [#LC0561]

- Las ventanas de las aplicaciones pueden redibujarse de forma incorrecta en las configuraciones de varios monitores.

  [#LC0600]

Interfaz de usuario

- Cuando la ventana de Receiver Store se cierra durante el inicio de la aplicación, la barra de progreso puede permanecer visible tras el inicio de la aplicación.

  [#LC0464]

- Al iniciar una aplicación o un escritorio, el cuadro de diálogo de inicio sigue vacío durante varios segundos sin ninguna descripción de actividad.

  [#LC0624]

- Esta corrección elimina un error tipográfico de la plantilla de administración predeterminada.

  [#LC0848]

Otros problemas

- Esta mejora de características en el registro del instalador de Citrix Receiver le permite:

  - Guardar registros en una ubicación permanente
  - Conservar el historial de instalación después de cada instalación
  - Recopilar información de los entornos de usuario antes de que se inicien las instalaciones reales
  - Proporcionar más información de depuración en los registros de instalación

  [#LA4615]

- Ahora CtxCredApi.dll y CtxCredApi(64).dll se incluyen en el paquete MSI de Citrix Receiver para Windows Enterprise. Ahora la API respalda 64 bits. Use CtxCredApi64.dll para las aplicaciones de 64 bits.

  [#LA4630]

- La utilización de CPU de todos los procesos de wfica de un servidor puede aumentar un 10 % cuando solo un usuario utiliza sonido en la sesión de usuario.

  [#LA5918]

- Es posible que Receiver no pueda leer correctamente el nombre de la organización de un certificado si el nombre contiene caracteres especiales, especialmente si se trata de caracteres que no pertenecen a los primeros 128 caracteres del juego de caracteres ASCII.

  [#LC0801]

- Al usar el comando "wfica32.exe /setup", el complemento ActiveX de wfica.ocx no puede registrar Internet Explorer.

  [#LC0927]

Nota: Esta versión de Citrix Receiver también incluye todas las soluciones que se incluyeron en las versiones 4.1 y 4.0.